REDES DE COMUNICAÇAO

Conceitos de Redes

Meios de Transmissão

Como as redes foram criadas com o propósito de transmitir dados vejamos a seguir os meios de transmissão de dados disponíveis:

Simplex – A transmissão de dados ocorre de maneira simples, ou seja, unidirecional, em uma única direção, existe um transmissor e um receptor e esse papel não se inverte. Como exemplos de transmissão simplex tem-se o rádio AM/FM e a TV não interativa.

Half-duplex – Esse tipo de transmissão de dados é bidirecional, ou seja, o emissor pode ser receptor e vice-versa, mas, por compartilharem um mesmo canal de comunicação, não é possível transmitir e receber dados ao mesmo tempo. Exemplo de transmissão half-duplex: rádio amador, walkie-talkie (as duas pessoas podem conversar mas só uma de cada vez). A maioria das placas de rede transmitem de modo half-duplex.

Full-duplex – Esse tipo de transmissão de dados é bidirecional porém, na transmissão full (completo) os dados podem ser transmitidos simultaneamente, ou seja, ao mesmo tempo que existe o envio pode existir o recebimento de informações. Exemplos de transmissão full-duplex: Aparelho telefônico. Com o crescente barateamento dos equipamentos de rede esta cada vez mais comum encontrar placas de rede que usam esse tipo de comunicação.

Meios de Comunicação

Depois de estudar o modo como a informação será transmitida o passo seguinte é estudar como as redes podem ser conectadas. A comunicação entre as redes pode ser feita do seguinte modo:

- Via Satélite;
- Via Rádio
- Via Cabo:
  - Cabo Fibra Ótica;
  - Cabo Elétrico;
  - Linha Telefônica – dedicada ou discada;

O meio de comunicação mais comum entre as redes de computadores e entre uma rede e a internet é a comunicação via linha telefônica e os tipos mais comuns são:

	Equipamentos	**Conexão**
Discada (Dial-up)	Modem Fax	Até 56 Kbps
Dedicada (ADSL)	Modem ADSL Placa de Rede	128 Kbps até 10Mbps

Técnicas de Comutação

Discutiremos agora as técnicas de comutação existentes para transporte de dados através de uma rede, suas características e a escolha do ATM como técnica mais adequada para a RDSI-FL. Na figura abaixo, livro do Stallings, tem-se uma representação das diversas técnicas de comutação em forma de espectro limitado em seus extremos pelas técnicas mais comuns de comutação de circuitos. As técnicas de comutação de circuitos e as outras situadas próximas deste extremo possuem como característica uma taxa de transmissão fixa e facilidade de implementação, enquanto que as técnicas que tendem a se situar para o lado direito do espectro têm facilidades de operação a taxas variáveis mas, por sua vez, são mais difíceis de serem implementadas.

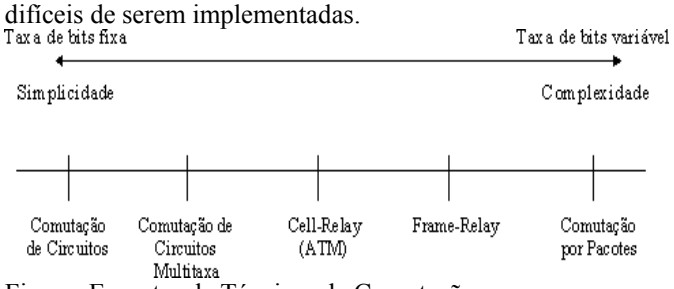


Figura: Espectro de Técnicas de Comutação

Comutação de Circuitos (Circuit Switching)

A comutação de circuitos implica na existência de um caminho dedicado para comunicação entre duas estações, com uma taxa de transmissão fixa. A comunicação via comutação de circuitos envolve três etapas: - estabelecimento da conexão; - transferência da informação; - desconexão do circuito;

Há a alocação de um canal que permanece dedicado à conexão até a sua desconexão (feita por um dos usuários através de sinais de controle). Para o caso de tráfego variável, este canal pode estar sendo subutilizado e para o tráfego em rajadas há um melhor rendimento na utilização de uma técnica de comutação por pacotes. Isso faz com que esta técnica seja muito utilizada na transmissão de voz (telefonia) e, conseqüentemente na RDSI-FE, que possui as características necessárias de taxa de transmissão constante (64 kbps) e tráfego contínuo.

Comutação de Circuitos Multitaxa (Multirate Circuit Switching)

A técnica de comutação de circuitos multitaxa nada mais é do que uma melhora da comutação de circuitos visando eliminar o desperdício da capacidade do canal alocado. Isto ocorre porque a conexão é feita através de vários circuitos simultaneamente. Apesar desta técnica apresentar uma boa melhora em termos de flexibilidade, podendo suportar serviços de diversas taxas, ainda não é uma opção adequada ao tráfego em rajadas.

Comutação de Pacotes (Packet Switching)

As técnicas de comutação de circuitos apresentam alto rendimento quando utilizadas em telefonia para transmissão de voz, pois o canal está ocupado quase que todo o tempo de conexão (um dos usuários está sempre falando). Porém, com o aumento da utilização da rede telefônica para a transmissão de dados, ocorrem alguns problemas, como por exemplo, a característica de variação da taxa na transmissão de dados e o dimensionamento da linha com base na taxa de pico, provocando subutilização da rede quando a taxa for menor. Esses incovenientes são evitados pelas técnicas de comutação de pacotes. Nesta técnica, quadros de informação são transmitidos por rotas definidas nó a nó, não havendo necessidade de

estabelecimento de um caminho dedicado entre as estações. Isso implica em um maior aproveitamento das linhas de comunicação, uma vez que os canais podem ser compartilhados por várias mensagens ao longo do tempo (as mensagens são transmitidas por demanda). Um dos mais graves problemas desta técnica é que os cabeçalhos dos pacotes são excessivamente grandes e isso dificulta a sua aplicação onde se tem altas taxas de transmissão. Além disso, como cada pacote a ser transmitido é armazenado e transmitido apenas quando o canal não está ocupado, quando o tráfego na rede é grande podem haver altos retardos entre pacotes, o que não é desejável para aplicações como voz, que exigem taxa constante de transmissão.

Frame-Relay

O frame-relay procura tirar proveito da qualidade dos atuais meios de transmissão. Como as transmissões estão se tornando cada vez mais confiáveis, o frame-relay consiste em eliminar grande parte do cabeçalho do packet-switching relacionado com o controle de erros. Desta forma, o frame-relay consegue atingir taxas de mais de 2 Mbps, enquanto o packet-switching se limita aos 64 kbps originais.

Comutação por Células (Cell-Relay)

O cell-relay pode, de certa forma, ser considerado o próprio ATM. Ele é uma combinação das características inerentes à comutação por circuitos e por pacotes, uma mistura equilibrada dos desenvolvimentos obtidos por essas duas tecnologias, utilizando o que cada uma possui de melhor. Em comparação ao frame-relay, o cell-relay possui as mesmas características de não-existência de controle nó a nó. Sua principal diferença é utilizar células de tamanho fixo, que possuem maior desempenho em termos de velocidade comparadas às células de tamanho variáveis, podendo trabalhar com taxas da ordem de até centenas de Mbps (enquanto o frame-relay atinge até 2 Mbps). Além dos vários canais lógicos que podem ser multiplexados sobre um único meio físico, o ATM faz uso de canais e caminhos virtuais. Ele pode ser comparado a uma técnica de comutação de circuitos multitaxa, porém nela os canais virtuais possuem suas taxas dinamicamente definidas no momento da conexão, diferindo dos canais de taxa fixa. Outro fator importante a ser considerado é o tamanho das células. Este fator provém de uma relação de compromisso entre a eficiência da transmissão, complexidade da rede e atraso. Após muita discussão, foi padronizado um valor de célula de 48 octetos como o ideal.

Estrutura Física

Existem diversos tamanhos e tipos de redes, mas o ponto de partida para elas é o mesmo: a necessidade de comunicação entre dois ou mais computadores. As formas de conexão podem ser as mais variadas, desde pares de cabos e de baixo custo, passando pelos cabos coaxiais e fibras óticas até equipamentos sem fio. Há ainda outros componentes utilizados para expandir a capacidade da rede. Entre esses componentes, podemos destacar:

Servidor: máquina central responsável por disponibilizar recursos e serviços na maioria das redes. Sua função á agir como fonte de dados para as configurações da rede, armazenamento de dados e plataforma para rodar aplicativos, além de possuir mecanismos de autenticação e controle de acesso – evitando assim que usuários acessem recursos não autorizados. Existem diversos tipos de servidores, a escolha depende da necessidade e do tamanho da rede em que será instalado. Exemplos de servidores: Servidor de arquivos, servidor de impressão, servidor de aplicações, servidor de correio eletrônico, servidor de fax, servidor de comunicação.

Cliente: é a máquina que utilizará a rede em questão. É com ela que o usuário vai acessar os recursos disponíveis, como serviços, programas e dispositivos de armazenamento no servidor, em outras maquinas cliente ou em dispositivos autônomos como fax ou impressoras remotas.

Cabos: são o meio físico por meio dos quais os dados serão transmitidos. Existem diversos tipos de cabos, e sua escolha vai depender do tipo de rede a ser instalada, do equipamento que será utilizado e de quanto o dono da rede esta disposto a gastar.

Interface de rede: hardware responsável pela conexão entre as máquinas, agindo como porta de entrada e saída para acesso ao "espaço público" da rede.

A estrutura física de uma rede de computadores com relação a sua abrangência pode ser dividida em:

***LAN (Local Área Network)* –** É um conjunto de computadores ligados em uma pequena região. São sinônimos de Rede LAN – **Rede Local, Rede Interna, *Ethernet*, Intranet.**

***MAN (Metropolitan Área Network)* –** É uma rede que visa cobrir uma área urbana com aproximadamente 30 Km de raio. Normalmente é composta pela interligação de todas as redes locais de uma mesma empresa, na mesma região metropolitana.

WAN (Wide Área Network) – É um conjunto de computadores ligados a grandes distâncias. Seu sinal é reforçado sempre para que não haja perda nos dados durante a transmissão dos mesmos. No caso de redes privadas, uma WAN é a interligação das MANs de uma mesma instituição ou grupo de instituições. Em se tratando de redes públicas, a WAN mais conhecida do mundo é a Internet.

Outros termos comuns usados são:

→**INTERNET –** Rede mundial de computadores.

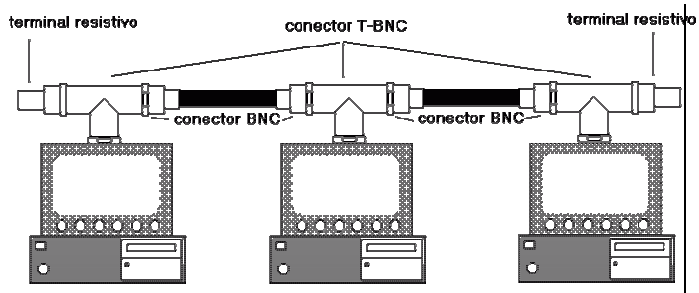
→**INTRANET –** Rede local que usa a mesma estrutura da Internet para o acesso de dados na rede.

→**EXTRANET –** Uma intranet que permite acesso remoto, isto é, que pessoas tenham acesso a ela através de um modem.

Topologia de redes de computadores

Uma rede de computadores pode ser dividida de acordo com as seguintes topologias:

Topologia em Barramento (backbone)



Esta topologia é constituída por uma linha única de dados (o fluxo é serial), finalizada por dois terminadores (casamento de impedância), na qual atrelamos cada nó de tal forma que toda mensagem enviada passa por todas as estações, sendo reconhecida somente por aquela que esta cumprindo o papel de destinatário (estação endereçada). Nas redes baseadas nesta topologia não existe um elemento central, todos os pontos atuam de maneira igual, algumas vezes assumindo um papel ativo outras vezes assumindo um papel passivo, onde a espinha dorsal da rede (backbone) é o cabo onde os computadores serão conectados. As redes locais Ethernet ponto-a-ponto usam essa topologia.

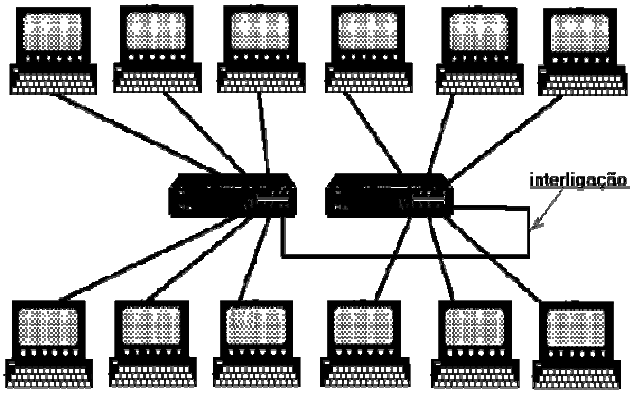
Vantagens – Solução de baixo custo, sendo ideal quando implementada em lugares pequenos.

Desvantagens – Como todas as estações estão atreladas a uma linha única (normalmente um cabo coaxial), o número de conexões é muito grande, logo, se a rede estiver apresentando um problema físico, são grandes as chances deste problema ser proveniente de uma dessas conexões (conectores e placas de rede) ou até mesmo de um segmento de cabo. A maior dificuldade esta em localizar o defeito, já que poderão existir vários segmentos de rede.

Como a troca de informações dá-se linear e serialmente, quando ocorrem tais defeitos toda a rede fica comprometida e para de funcionar.

A ampliação da rede, com a inclusão de novas estações e/ou servidores implica na paralisação da estrutura de comunicação.

Topologia em Estrela



A topologia em estrela é caracterizada por um elemento central que "gerencia"o fluxo de dados da rede. Toda informação enviada de um nó para outro deverá obrigatoriamente passar pelo ponto central, ou concentrador, tornando o processo muito mais eficaz, já que os dados não irão passar por todas as estações. O concentrador encarrega-se de rotear o sinal para as estações solicitadas, economizando tempo. Existem também redes estrela com conexão passiva (similar ao barramento), na qual o elemento central nada mais é do que uma peça mecânica que atrela os "braços"entre si, não interferindo no sinal que flui por todos os nós, da mesma forma que o faria em redes com topologia barramento.

Vantagens – Alta performance, uma vez que o sinal sempre será conduzida para um elemento central, e a partir deste para o seu destino, as informações trafegam bem mais rápido do que numa rede barramento.

Facilidade na instalação de novos segmentos ou de inclusão de nova estação na rede, bastando apenas conectá-las ao concentrador.

Facilidade de isolar a fonte de uma falha de sistema ou equipamento, uma vez que cada estação está diretamente ligada ao concentrador.

A ocorrência de falhas em um segmento não retira toda a estrutura do ar.

Desvantagens – Custo elevado de instalação, sendo que quanto maior for a distância entre um nó e o concentrador maior será o investimento, já que cada "braço"é representado por um segmento de cabo coaxial, par trançado ou fibra óptica.

Problemas de confiabilidade, já que uma falha no concentrador, no caso de redes sem redundância, provoca a perda de comunicação em toda a rede.

Todo o tráfego flui através do concentrador, podendo representar um ponto de congestionamento.

Topologia em Anel – A topologia anel é constituída de um circuito fechado que permite a conexão de vários computadores em círculo (anel) e por isso não possui pontas, as informações nesse tipo de rede se propagam através de todos os computadores em um determinado sentido (horário).

Vantagens – Não há atenuação do sinal transmitido, já que ele é regenerado cada vez que passa por uma estação (a atenuação é diretamente proporcional à distância entre um nó e outro).

Possibilidade de ter dois anéis funcionando ao mesmo tempo, onde caso exista falha em um, somente ocorrerá uma queda de performance.

Desvantagens – Todas as estações devem estar ativas e funcionando corretamente.

Dificuldade de isolar a fonte de uma falha de sistema ou de equipamento.

Ampliação da rede, inclusão de novas estações ou servidores implica na paralisação da rede.

Redes de Computadores – Cabeamento

1 – CABO COAXIAL

Foi o primeiro tipo de cabo empregado nas redes de computadores. É constituído de um condutor interno cilíndrico no qual o sinal é injetado, um condutor externo separado do condutor interno por um elemento isolante e uma capa externa que evita a irradiação e a capacitação de sinais. Tipo de cabo muito utilizado na rede do tipo Barramento. Características de um cabo coaxial:

Thinnet – Cabo Coaxial Fino (**10base2**)

Impedância de 50Ω;
Coprimento máximo 200m (teoria) 185m (Prática);
10 Mbps de taxa de transferência;
Taxa de Transmissão de 1 a 50 Mbps (depende do tamanho do cabo);
Transmissão Half Duplex;
Limite de 30 equipamentos / segmento;
Conector **T**.

Thicknet – Cabo Coaxial Grosso (**10base5**)
Impedância de 75Ω;
Comprimento máximo 500m;
10 Mbps de taxa de transferência;
Taxa de Transmissão de 100 a 150 Mbps (depende do tamanho do cabo);
Transmissão Full Duplex;
Conector: esse cabo é conectado à placa através de um transceiver (transceptores que detectam a portadora elétrica do cabo).

Conectores para Cabo Coaxial

Conector BNC

Terminador Resistivo BNC

Conector T-BNC

O conector para os cabos Thinnet e Thicknet é o conector **BNC** (British Naval Connector) Conector Naval Britânico, podendo ser o *plug BNC ou T – BNC.*

DESVANTAGENS DO CABO COAXIAL:

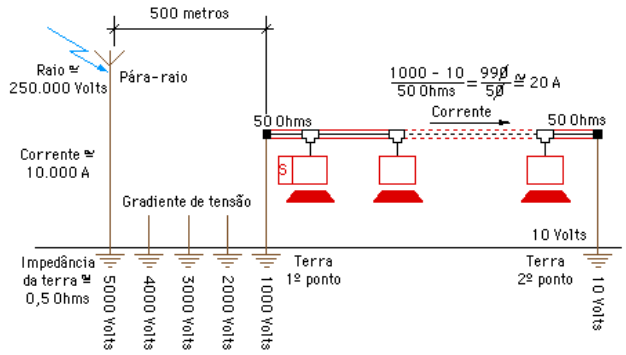
1. Necessita manter a impedância constante, através de terminadores.

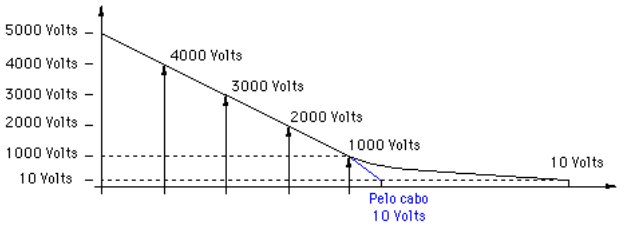
2. Se o cabo quebrar, ou o "T" de interligação estiver com mau contato, a Rede à partir do ponto falho irá parar.

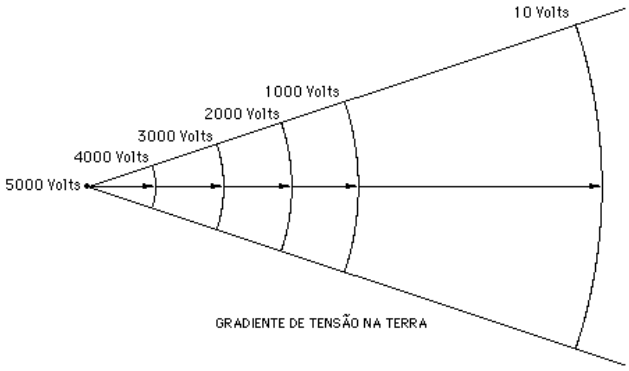
3. Blindagem feita com a malha do cabo, que deverá estar aterrada em todos os terminais, ocasionando diferentes potenciais elétricos. A blindagem acaba funcionando como uma antena captando ruído de rádio freqüência.

4. Se esta blindagem for aterrada num ponto do edifício, e em outro ponto à 100 m do 1º ponto, com certeza esta blindagem terá potenciais diferentes, ocasionando correntes elétricas pela malha entre os micros.

5. Nesta condição, se uma descarga atmosférica ocorrer próxima à 500m do 1º ponto, elevará o potencial do Terra, do 1º ponto a um valor muito maior que o do 2º ponto à 100m, gerando um pico de tensão pelo cabo, do ponto 1º ao ponto 2º, com potencial de até 1.000Volts, queimando diversos terminais e até mesmo o servidor.







6. É um cabo muito pesado e de difícil de Instalação.

2 – CABO PAR TRANÇADO

Existem dois tipos básicos de cabos par trançado:
UTP - Unshielded Twisted Pair - Par trançado sem blindagem.

O cabo UTP é o mais utilizado em rede, o cabo UTP é de fácil manuseio, instalação e permite taxas de transmissão em até 100 Mbps com a utilização do cabo CAT 5 são usados normalmente tanto nas redes domesticas como nas grandes redes industriais e para distancias maiores que 150 metros hoje em dia é utilizados os cabos de fibra ótica que vem barateando os seus custos.

O CABO UTP

Os cabos UTP foram padronizados pelas normas da EIA/TIA com a norma 568 e são divididos em 5 categorias, levando em conta o nível de segurança e a bitola do fio, onde os números maiores indicam fios com diâmetros menores, veja abaixo um resumo simplificado dos cabos UTP.

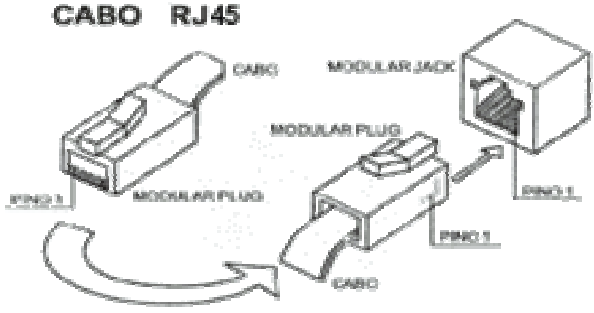
Tipo	Uso	
Categoria 1	Voz (Cabo Telefônico)	São utilizados por equipamentos de telecomunicação e não devem ser usados para uma rede local
Categoria 2	Dados a 4 Mbps (LocalTalk)	
Categoria 3	Transmissão de até 16 MHz. Dados a 10 Mbps (Ethernet)	
Categoria 4	Transmissão de até 20 MHz. Dados a 20 Mbps (16 Mbps Token Ring)	
Categoria 5	Transmissão de até 100 MHz. Dados a 100 Mbps (Fast Ethernet)	
Categoria 6	Transmissão com taxas típicas de até 1Gbps.	

STP - Shielded Twisted Pair - Par trançado com blindagem.

O cabo brindado STP é muito pouco utilizado sendo basicamente necessários em ambientes com grande nível de interferência eletromagnética. Deve-se dar preferência a sistemas com cabos de fibra ótica quando se deseja grandes distâncias ou velocidades de transmissão, podem ser encontrados com blindagem simples ou com blindagem par a par. Os cabos STP são classificados em 1, 1A, 2A, 6, 6A, 9, 9A. Os cabos STP projetados para redes podem ser:

- *STP de 100 ohms:* Aumenta a resistência contra interferência eletromagnética do fio de par trançado sem fazer com que o cabo seja maior e mais pesado. O cabo precisa de um sistema de aterramento adequado, caso contrário passa a funcionar como antena causando grandes transtornos para a rede.
- *STP de 150 ohms:* Cabo que possui uma blindagem especial, sendo cada par de fios trançados separados por uma blindagem. Com toda essa blindagem o cabo fica mais pesado e seu custo é mais elevado.

Os conectores para cabo Par Trançado



Os conectores para Par Trançado são o RJ45 (permite a conexão de 8 fios) para redes de dados e conector de RJ11 (permite a conexão de 4 fios) usando em telefonia.

VANTAGENS DO CABO UTP:

1. Não tem blindagem, portanto não necessita de Aterramento.

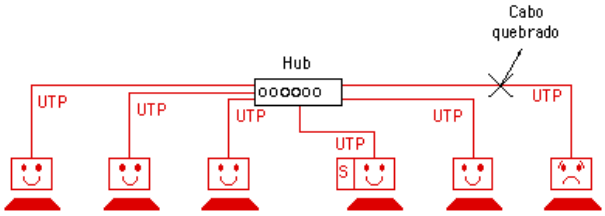
2. Mantém impedância constante de 100 OHMS sem terminadores.

3. Cabo leve, fino, de baixo valor por metro (R$0,70) e de conectores baratos para 8 (oito) contatos. (R$0,90)

4. No cabeamento estruturado para o cabo UTP, quando há mal contato ou o cabo é interrompido, apenas um micro pára de funcionar, enquanto o resto da Rede continua funcionando normalmente.

5. Permite taxas de Transmissão da ordem de 155 Mb/s por par.

6. Alcança velocidades de 155Mb/s à 622Mb/s ATM ou FAST ETHERNET 100Mb/s.



Além do cabo UTP, as pesquisas levaram à criação da fibra óptica, um tarugo de 10cm de quartzo (cristal), que é estirado até alcançar um comprimento de 2Km à 20Km, com uma espessura de um fio de cabelo, capaz de transmitir dados em forma de luz, internamente a uma velocidade de aproximadamente 2.500Mb/s ou mais (não há aparelhos hoje acima desta velocidade).

A fibra óptica pode trafegar livre de interferência e de espúrios atmosféricos, sem blindagem e sem aterramento.

Com estes novos componentes as empresas americanas EIA/TIA criaram normas para as Redes de Computadores (telefonia e imagem).

A Norma EIA/TIA 568 A, garante comunicação de dados até 100m para o cabo UTP, à velocidades de 100Mb/s (categoria 5) que é o nosso estado da arte (atualmente), e 2.500Mb/s para fibras até 2.500m (mult modo) e 60.000m (mono modo).

Segundo o modelo ISO/OSI, o Ethernet é o padrão que define os níveis 1 e 2 (físico e lógico) especificados pelas normas 802.3 e 802.2 IEEE.

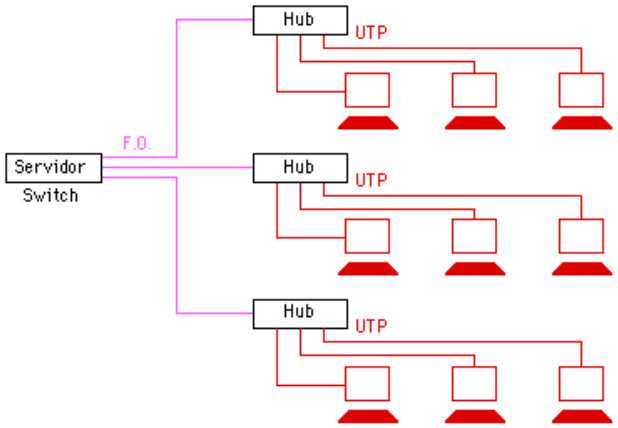
O cabo UTP garante 155Mb/s por par, ou seja, 4 x 155Mb/s = 622Mb/s, pois tem 4 (quatro) pares.

Este é o cabeamento estruturado, pois pode trafegar a qualquer velocidade, desde 0,1MHz à 100MHz, atendendo todas as categorias: cat. 3 (10 Mhz), cat. 4 (até 20 Mhz), substituída pela cat. 5 (100 Mhz).

Desta forma, o cabeamento de uma empresa se resume em:

1 - Rede Principal ou Back Bone, em fibra óptica.

2 - Rede Horizontal, em cabo UTP cat. 5.



Com esta Topologia é possível interligar pilhas de Hubs (100MHz) ou Switch, e manter a velocidade de 100Mb/s até o servidor, sem gargalo.

PADRÃO EIA/TIA 568

1.1. Introdução

No final dos anos 80, as companhias dos setores de telecomunicações e informática estavam preocupadas com a falta de uma padronização para os sistemas de fiação de telecomunicações em edifícios e campus.

Em 1991, a associação EIA/TIA (Electronic Industries Association / Telecommunications Industry Association) propôs a primeira versão de uma norma de padronização de fios e cabos para telecomunicações em prédios comerciais, denominada de EIA/TIA-568 cujo objetivo básico era:

a. Implementar um padrão genérico de cabeação de telecomunicações a ser seguido por fornecedores diferentes;

b. Estruturar um sistema de cabeação intra e inter predial, com produtos de fornecedores distintos;

c. Estabelecer critérios técnicos de desempenho para sistemas distintos de cabeação.

Até então, o mercado dispunha de tecnologias proprietárias, utilizando cabeação tradicional, baseado em aplicações, conforme ilustrado na Figura 1.

Assim, os prédios possuíam cabeação para voz, dados, sistemas de controle, eletricidade, segurança, cada qual com uma padronização proprietária. Eram fios e cabos por toda parte, cabo coaxial, par trançado, cabo blindado. Neste cenário, alguns problemas surgiram para desestimular essa forma de cabeação não estruturada:

i) Mudança rápida de tecnologia: microcomputadores (PCs) mais velozes, serviços integrados de voz e dados, redes locais de alta velocidade;

ii) Infra-estrutura de telefonia privada inadequada para novas tecnologias;

iii) Rápida saturação de dutos, canaletas e outros suportes de cabeação;

iv) Inflexibilidade para mudanças;

v) Cabeação não reaproveitável com novas tecnologias;

vii) Suporte técnico dependente de fabricantes;

viii) Aumento de custo.

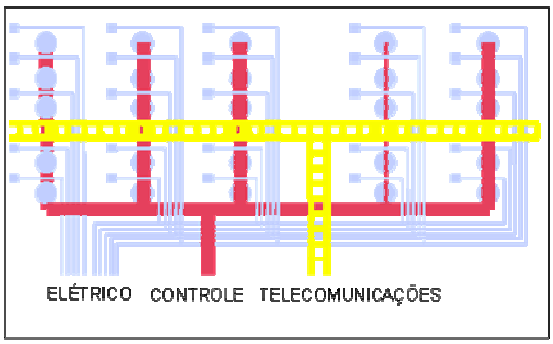


Figura 1: Cabeação com Sistemas de Fiação Separados

Em janeiro de 1994, a EIA/TIA publicou a norma EIA/TIA 568A revisada, incluindo as especificações para cabeação categoria 4 e 5 (UTP - Unshielded Twisted Pair). Atualmente, a associação ISO/IEC (International Standards Organization/International Electrotechnical Commission) desenvolve um padrão de cabeação internacional denominado de Cabeação Genérica para Instalação do Cliente (Generic Cabling for Customer Premises), denominado de ISO/IEC 11801. A norma ISO/IEC 11801 é equivalente à EIA/TIA 568A reeditada pela ISO.

1.2. Sistema de cabeação estruturada

O conceito de Sistema de Cabeação Estruturada baseia-se na disposição de uma rede de cabos, com integração de serviços de dados e voz, que facilmente pode ser redirecionada por caminhos diferentes, no mesmo complexo de cabeação, para prover um caminho de transmissão entre pontos da rede distintos. Um Sistema de Cabeação Estruturada EIA/TIA 568A é formado por seis subsistemas conforme ilustrado na Figura 2 e descritos a seguir.

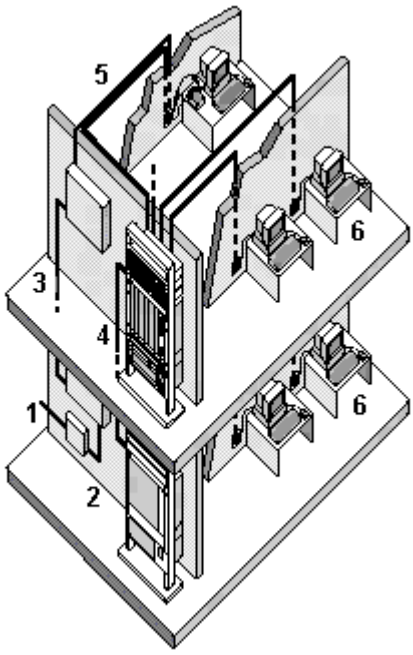


Figura 2: Sistemas de Cabeação Estruturada EIA/TIA 568

ENTRADA NO EDIFÍCIO

As instalações de entrada no edifício fornecem o ponto no qual é feita a interface entre a cabeação externa e a cabeação intra-edifício e consistem de cabos, equipamentos de conexão, dispositivos de proteção, equipamentos de transição e outros equipamentos necessários para conectar as instalações externas ao sistema de cabos local.

A norma associada EIA/TIA 569 define a interface entre a cabeação externa e a cabeação interna do prédio.

SALA DE EQUIPAMENTOS

A Sala de Equipamentos é o local propício para abrigar equipamentos de telecomunicações, de conexão e instalações de aterramento e de proteção. Ela também contém a conexão cruzada principal ou a conexão secundária, usada conforme a hierarquia do sistema de Cabeação Backbone.

A Sala de Equipamentos é considerada distinta do Armário de Telecomunicações devido à natureza ou complexidade dos equipamentos que elas contém. Qualquer uma ou todas as funções de um Armário de Telecomunicações podem ser atendidas por uma Sala de Equipamentos.

A norma associada EIA/TIA-569 define, também, o projeto da Sala de Equipamentos.

SUBSISTEMA DE CABEAÇÃO BACKBONE

O subsistema de Cabeação Backbone ou Cabeação Vertical, ilustrado na Figura 3, consiste nos meios de transmissão (cabos e fios), conectores de cruzamento (cross-connects) principal e intermediários, terminadores mecânicos, utilizados para interligar os Armários de Telecomunicações, Sala de Equipamentos e instalações de entrada.

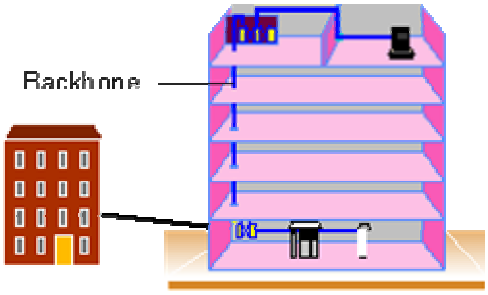


Figura 3: Subsistema de Cabeação Backbone

Os cabos homologados na norma EIA/TIA 568A para utilização como Backbone são:

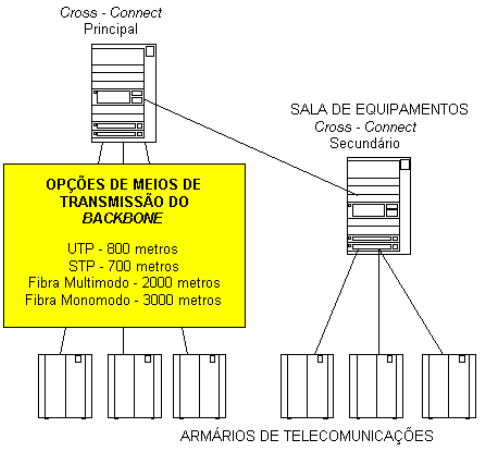
a. Cabo UTP de 100 Ohms (22 ou 24 AWG):
   - 800 metros para voz (20 a 300 MHz);
   - 90 metros para dados (Cat. 3,4 e 5).
b. Cabo STP (par trançado blindado) de 150 Ohms:
   - 90 metros para dados.
c. Fibra óptica multimodo de 62,5/125 m:
   - 2.000 metros para dados.
d. Fibra óptica monomodo de 8,5/125 m:
   - 3.000 metros para dados.

Para os cabos UTP de 100 Ohms e STP de 150 Ohms, o alcance da cabeação depende da aplicação. A distância de 90 metros para dados em STP é aplicada para largura de banda de 20 a 300 MHz. Por outro lado, na transmissão de dados numa largura de banda de 5 a 16 MHz, o cabo UTP, categoria 3, tem sua distância reduzida de 800 para 90 metros. A distância de 90 metros é aplicada, também, para as categorias 4 e 5 em larguras de banda de 10 a 20 MHz e 20 a 100 MHz, respectivamente.

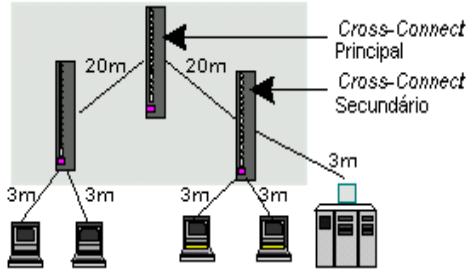
O subsistema de Cabeação Backbone define, também, outros requisitos de projeto, tais como:

a. Topologia em estrela;
b. Não possuir mais de dois níveis hierárquicos de conectores de cruzamento (cross-connect);
c. Os cabos que ligam os cross-connect não podem ultrapassar 20 metros;
d. Evitar instalações em áreas onde existam interferências eletromagnéticas e rádio freqüência;
e. As instalações devem ser aterradas seguindo a norma EIA/TIA 607.

a) Estrutura Geral



b) Configurações Limites



A Figura 4 ilustra a estrutura geral e as configurações limites para o subsistema de Cabeação Backbone.

ARMÁRIO DE TELECOMUNICAÇÕES

O Armário de Telecomunicações é o local, dentro de um prédio, onde são alojados os elementos de cabeação. Dentro do Armário de Telecomunicações são encontrados terminadores mecânicos, conectores de cruzamento (cross-connects), terminadores para os sistemas de Cabeação Horizontal e Vertical (patch panel).

SUBSISTEMA DE CABEAÇÃO HORIZONTAL

O subsistema de Cabeação Horizontal, ilustrado na Figura 5, compreende os cabos que vão desde a Tomada de Telecomunicações da Área de Trabalho até o Armário de Telecomunicações. O subsistema de Cabeação Horizontal possui os seguintes elementos:

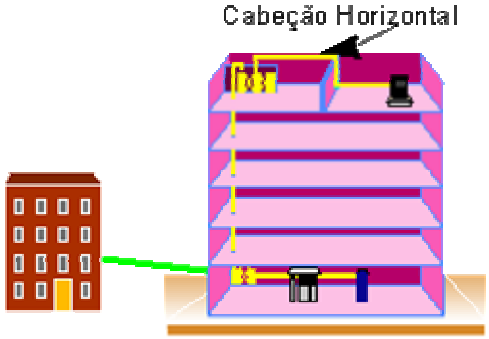
a. Cabeação Horizontal;

b. Tomada de Telecomunicações;

c. Terminações de Cabo;

d. Cross-Connections.

a) Cabeação Horizontal



b) Distâncias Limites

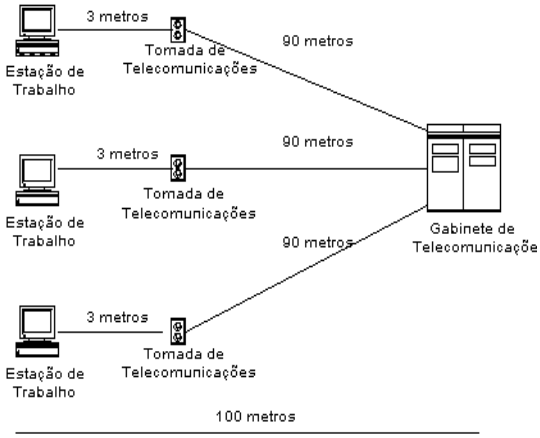
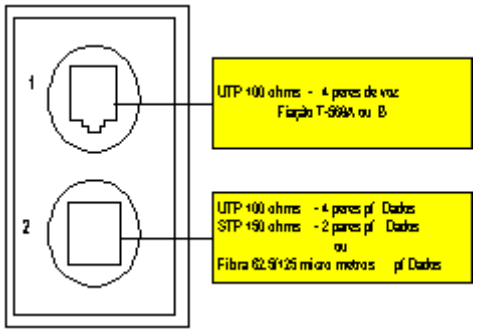


Figura 5: Subsistema de Cabeação Horizontal

c) Tomada de Telecomunicações


1
2
UTP 100 ohms - 4 pares de voz
Fiação T-568A ou B
UTP 100 ohms - 4 pares p/ Dados
STP 150 ohms - 2 pares p/ Dados
ou
Fibra 62.5/125 micro metros p/ Dados

O comprimento máximo para a Cabeação Horizontal, definido na norma EIA/TIA 568A, é de 90 metros, independente do meio de transmissão utilizado. A norma EIA/TIA 568A prevê, hoje, quatro tipos de cabos para instalação na Cabeação Horizontal:

a. Cabo com quatro pares de fios UTP de 100 Ohms;

b. Cabo com dois pares de fios STP de 150 Ohms;

c. Cabo coaxial de 50 Ohms;

d. Cabo com duas fibras ópticas multimodo 62,5/125m m.

Embora o cabo coaxial de 50 Ohms seja especificado na norma EIA/TIA-568A, existe uma tendência para que ele seja suprimido da próxima revisão. É aconselhável, hoje, que este tipo de cabo seja substituído em antigas instalações e não seja recomendado para instalações novas.

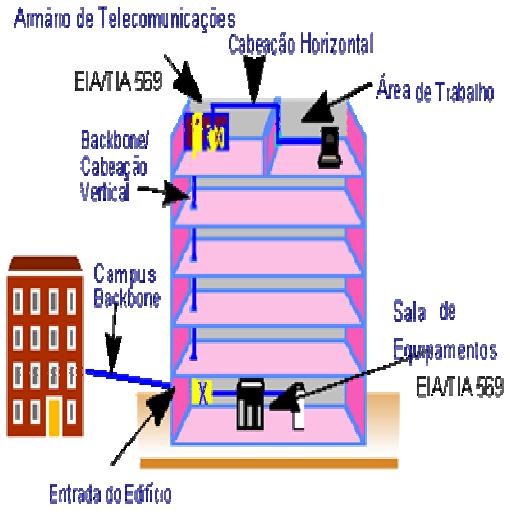
A norma prevê 100 metros total para a Cabeação Horizontal: 90 metros entre o Armário de Telecomunicações e as Tomadas de Telecomunicações (conectores de parede) [ver Fig. 5b e 5c]; 10 metros para cabos entre uma estação de trabalho e o conector de parede, (em geral, 3 metros) mais as conexões internas do Armário de Telecomunicações e entre este e os equipamentos ativos (7 metros restantes).

ÁREA DE TRABALHO

A norma EIA/TIA 568A estabelece que os componentes de cabeação entre a Tomada de Telecomunicações e a Estação de Trabalho devem ser simples, baratos e permitam flexibilidade de deslocamento, sem comprometer a conexão física. Os componentes da Área de Trabalho são:

a. Equipamento da estação: computadores, terminais de dados, telefone, etc.;
b. Cabos de ligação - cordões modulares, cabos de adaptação, jumpers de fibra;
c. Adaptadores.

a)



b)

1.3. Desempenho do hardware e meios de trasmissão

A norma EIA/TIA 568 classifica o sistema de cabeação em categorias levando em consideração aspectos de desempenho, largura de banda, comprimento, atenuação e outros fatores de influência neste tipo de tecnologia. A seguir, serão apresentadas as categorias de cabeação com tecnologia de par trançado UTP e STP e de fibra óptica.

CABEAÇÃO UTP

Os cabos UTPs são compostos de pares de fios trançados não blindados de 100 Ohms. Este tipo de cabo, nos dias de hoje, são projetados para alto desempenho na transmissão de dados ou voz.

Tipos de Cabo UTP

O cabo UTP pode ser classificado em três categorias como mostrado abaixo:

a. Categoria 3 - Utiliza cabos com pares de fios trançados sólidos de bitola 24 AWG. Os fios AWG24 apresentam uma impedância típica de 100 Ohms, a 16 MHz. Estes cabos são utilizados para transmissão de sinais até 16 MHz.
b. Categoria 4 - Utiliza cabos com pares de fios trançados sólidos de bitola 22 ou 24 AWG, com impedância de 100 Ohms a 20 MHz. Este cabos são utilizados para transmissão até uma largura de banda de 20 MHz;
c. Categoria 5 - Utiliza cabos com pares de fios trançados sem blindagem de bitola 22 ou 24 AWG e impedância de 100 Ohms a 100 MHz. Este tipo de categoria é recomendável para aplicações com taxa de transmissão elevada, por exemplo, para transmissão de imagens e dados a 100 Mbps.

Desempenho

A atenuação é comumente derivada da medida do sinal de varredura da frequência na saída de um cabo de comprimento maior ou igual a 100 metros (328 ft), ou seja, é a perda de potência do sinal no meio, em função da distância a uma determinada freqüência.

As perdas por diafonia ou NEXT são comumente derivadas de medidas de varredura de freqüência. Por exemplo, na comunicação de voz, seus efeitos são sentidos por linhas cruzadas, isto é, vozes estranhas que são escutadas durante uma ligação telefônica.

A perda NEXT decresce com o aumento da freqüência conforme a fórmula abaixo:

NEXT(f) ³ NEXT(0,772) - 15 log (f/0,772)

Desempenho do Cabo UTP na Cabeação Horizontal e Backbone

A impedância característica do cabo UTP para Cabeação Horizontal e Backbone é de 100 Ohms + 15% de 1 MHz até a maior freqüência da categoria (16, 20 ou 100 MHz);

A Figura 6 apresenta um comparativo entre as três categorias UTP (3, 4 e 5) quanto a atenuação e perdas por diafonia (crosstalk ou NEXT), no caso de uso na Cabeação Horizontal e na Cabeação Backbone.

a) Cabeação Horizontal e Backbone UTP

Frequência (MHz)	**Cat. 3 Atenuação (dB)**	**Cat. 4 Atenuação (dB)**	**Cat. 5 Atenuação (dB)**
1,0	2,6	2,2	2,0
4,0	5,6	4,3	4,1
8,0	8,5	6,2	5,8
10,0	9,7	6,9	6,5
16,0	13,1	8,9	8,2
20,0	-	10,0	9,3
25,0	-	-	10,4
31,25	-	-	11,7
62,5	-	-	17,0
100,0	-	-	22,0
Atenuação : [por 100 metros (328 pés) @ 20° C]			

b) Curva de Freqüência x Atenuação

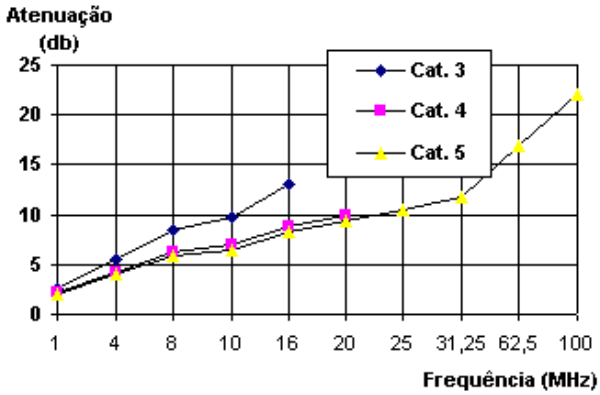


Figura 6: Desempenho de Atenuação x Freqüência para Cabos UTP em Cabeação Horizontal e Backbone

O gráfico da Figura 6(b) mostra que a atenuação em cabos categoria 3 e 4 é ligeiramente superior que a categoria 5 nas mesmas freqüências de trabalho. Verifica-se, aqui, a melhor qualidade dos cabos UTPs categoria 5 para redes Ethernet de 10 a 100 Mbps quanto às perdas por atenuação.

Desempenho dos Cordões e Hardware de Conexões UTP

Os Terminadores para cabo UTP devem utilizar contatos por deslocamento por isolador (IDC). Os limites máximos para jumper/cordões de ligação são:

i) 20 m para cross-connect principal;
ii) 20 m para cross-connect intermediário;
iii) 6 m no armário de telecomunicações;
iv) 3 m na estação de trabalho.

O desempenho do hardware de conexões UTP na Área de Trabalho é comparado na Figura 7.

a) Atenuação

Freqüência (MHz)	**Cat. 3 Atenuação (dB)**	**Cat. 4 Atenuação (dB)**	**Cat. 5 Atenuação (dB)**
1,0	0,4	0,1	0,1
4,0	0,4	0,1	0,1
8,0	0,4	0,1	0,1
10,0	0,4	0,1	0,1
16,0	0,4	0,2	0,2
20,0	-	0,2	0,2
25,0	-	-	0,2

31,25	-	-	0,2
62,5	-	-	0,3
100,0	-	-	0,4
Atenuação : [por 100 metros (328 pés) @ 20° C]			

b) Curva de Freqüência x Atenuação

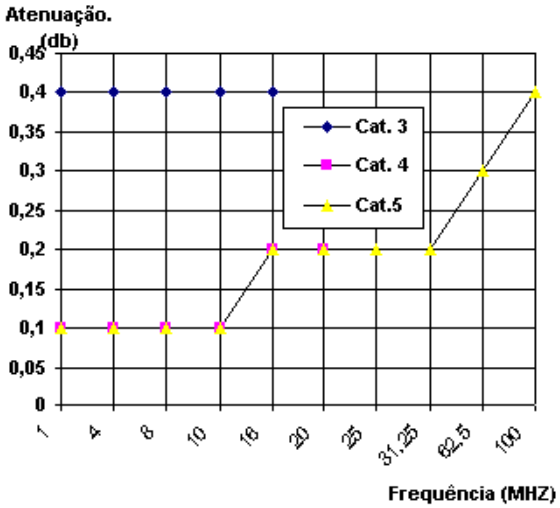


Figura 7: Desempenho do Hardware de Conexão UTP

O gráfico da Figura 7 mostra altas taxas de atenuação para os elementos de hardware da categoria 3 em determinada freqüência, por exemplo 16 MHz. Observa-se também, na figura 7, que perdas por atenuação em elementos de conexão, para categoria 4 e 5, são praticamente idênticas e bem inferiores às da categoria 3. Por causa do melhor desempenho de Elementos de Conexão nas categorias 4 e 5, deve-se, dar preferência a estas categorias de elementos quando da concepção de um projeto de cabeação estruturada. Na montagem dos condutores de ligação (patch-cords) deverão ser utilizados condutores não rígidos para maior duração e flexibilidade.

A terminação dos cabos horizontais deverá ser feita com material de conexão da mesma categoria ou superior do cabo UTP utilizado na Cabeação Horizontal. Por outro lado, os cabos utilizados para cordões de ligação e jumpers de cross-connect devem pertencer à mesma categoria do cabo UTP usado na Cabeação Horizontal.

Um sistema de cabeação UTP só poderá ser classificado como categoria 3, 4 ou 5 se todos os componentes do sistema de cabeação atenderem aos requisitos da categoria.

A Figura 8 ilustra o desempenho dos cordões de ligação UTP.

a) Atenuação Máxima

Frequência (MHz)	**Cat. 3 Atenuação (dB)**	**Cat. 4 Atenuação (dB)**	**Cat. 5 Atenuação (dB)**
1,0	3,1	2,6	2,4
4,0	6,7	5,2	4,9
8,0	10,2	7,4	6,9
10,0	11,7	8,3	7,8
16,0	15,7	10,7	9,9
20,0	-	12,0	11,1
25,0	-	-	12,5
31,25	-	-	14,1
62,5	-	-	20,4
100,0	-	-	26,4

b) Curva de Freqüência x Atenuação

Atenuação : [por 100 metros (328 pés) @ 20° C]

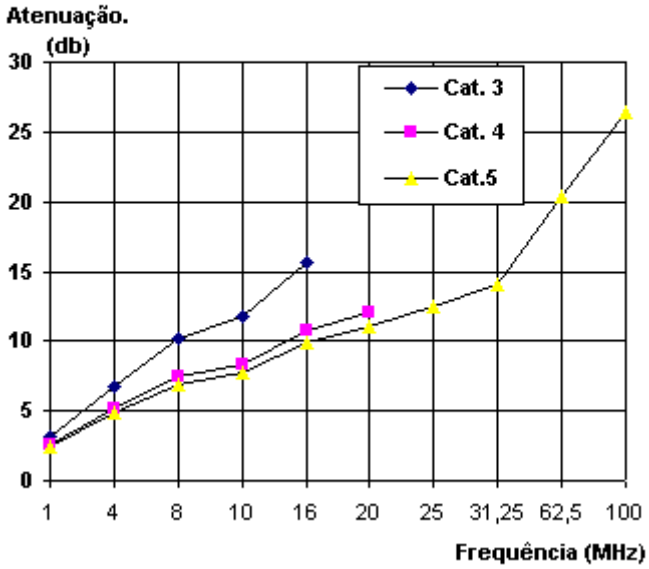


Figura 8: Desempenho dos Cordões de Ligação UTP

CABEAÇÃO STP

Quando as especificações para cabeação STP (Shielded Twisted Pair) de 150 Ohms foram publicadas na norma EIA Interim Standard Omnibus Specification NQ-EIA/IS-43, as características de transmissão aceitavam sinais de até 20 MHz. Estas especificações têm sido adequadas até o presente momento para faixas de freqüências usadas em ambientes de trabalho. Entretanto, como a velocidade das LAN's e suas freqüências aumentaram, as especificações originais dos cabos STP de 150 Ohms foram aumentadas de modo a prover um critério de desempenho estável para valores altos de freqüência aplicados. Um cabo de especificação melhorada e um novo conector, acoplado ao conector original foi introduzido para atender as especificações originais.

Os cabos STP são de fios em pares trançados blindados de 150 Ohms. Para a Cabeação Horizontal e a Backbone são utilizados os tipos 1A e o tipo 6A da IBM para cabos de conexão, cujas características são as seguintes:

a. Cabo STP-A utiliza 2 pares de fios, modelo 22 AWG rígido e possui impedância característica de 150 Ohms ± 10% (3 MHz - 300 MHz);
b. O conector de dados STP-A de 150 Ohms;
c. A atenuação balanceada do Cabo de Ligação STP-A de 150 Ohms é aproximadamente igual a 1,5 vezes a do cabo STP-A Horizontal ou Backbone (4 MHz - 300 MHz).

A Figura 9 ilustra o desempenho dos cabos STP em termos de atenuação.

a) **Tabela** ° C]

Freqüência (MHz)	STP-A Horizontal e Backbone	STP-A de Ligação -150 Ohms
4,0	2,2	0,05
8,0	3,1	0,10
10,0	3,6	0,10
16,0	4,4	0,15
20,0	4,9	0,15
25,0	6,2	0,15
31,25	6,9	0,15
62,50	9,8	0,20
100,0	12,3	0,25
300,0	21,4	0,45

Atenuação : [dB por 100 metros (328 pés) @ 20

b) Gráfico

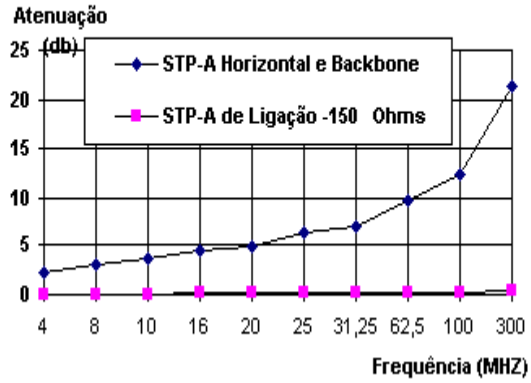


Figura 9: Atenuação X Freqüência em Cabos STP

FIBRA ÓPTICA

A fibra óptica pode ser utilizada tanto para a Cabeação Horizontal como para a Vertical. A fibra para Cabeação Horizontal é do tipo multimodo de 62,5/125m m com um mínimo de duas fibras. A Cabeação Vertical ou Backbone utiliza fibras dos tipos multimodo de 62,5/125m m e monomodo formados em grupos de 6 ou 12 fibras.

As premissas para uma Cabeação Backbone com fibra ópticas, têm sido e continuam a ser baseadas em fibras multimodo de 62,5/125m m, devido à possibilidade de uso de transmissores ópticos com LED nessas fibras. Com o rápido crescimento dos requisitos de largura de banda, atualmente, tem-se instalado fibras ópticas monomodo em adição às fibras multimodo, para atender os requisitos atuais e futuros. Sistemas de fibras monomodo atendem tanto maiores bandas de freqüências como também têm maior capacidade para longas distâncias do que as fibras ópticas multimodo.

a) Tipos de Fibra Óptica

b) Atenuação Máxima

Comprimento de Onda (nm)	Fibra Óptica multimodo (dB/Km)	Fibra Óptica Monomodo (dB/Km)
850	3,75	
1300	1,5	
1310		0,5
1550		0,5

c) Comprimento de Onda x Atenuação

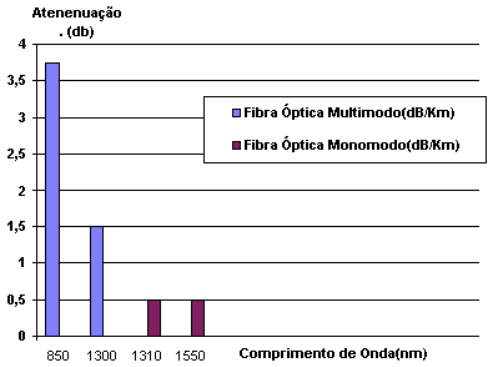


Figura 10: Desempenho da Cabeação com Fibra Óptica

Os conectores especificados para fibra óptica são os 568SC. Os conectores ópticos seguem um esquema de cores para sua identificação. A cor bege especifica o conector/acoplamento multimodo de 62,5/125m m e a cor azul especifica o conector/acoplamento monomodo de 8,3/125m m.

Para assegurar que os conectores 568SC manterão uma correta polarização através do sistema de cabeação, deve-se ter uma correta orientação do adaptador utilizado. A Cabeação Horizontal deve ser instalada de tal forma a casar um número ímpar da fibra com o próximo número par da fibra, por exemplo: fibra 1 com fibra 2; fibra 3 com fibra 4 e assim sucessivamente. Cada segmento da cabeação deve ser instalado seguindo a orientação invertida (cross-over) do par, de tal modo que fibras de número ímpar são posição A numa ponta e posição B na outra ponta, enquanto que fibras de número par são posição B numa ponta e posição A na outra ponta. A orientação invertida (cross-over) deve ser conseguida pelo uso consecutivo da numeração das fibras (por exemplo 1, 2, 3, 4, ...) em ambos os lados da fibra, mas os adaptadores 568SC devem ser instalados de maneira oposta em cada ponta (por exemplo A-B, A-B, ... numa ponta e B-A, B-A, ... na outra ponta). A Figura 11 ilustra a polarização inversa dos conectores 568SC.

O principal motivo para especificação dos conectores de fibra 568SC é a padronização com a norma IEC Européia. Hoje são muito utilizados conectores ST. Entretanto, é recomendado a substituição gradativa dos conectores ST por 568SC.

A norma EIA/TIA 568A especifica, também, as saídas de telecomunicações para fibra óptica com as seguintes características:

i) A caixa de montagem em superfície deve ser fixada diretamente sobre a caixa elétrica, seguindo um padrão de 4"x 4";
ii) A capacidade de terminação para um mínimo de duas fibras, por acoplamento 568SC;
iii) Possibilidade de armazenar um mínimo de 1 metro de cabo de duas fibras.

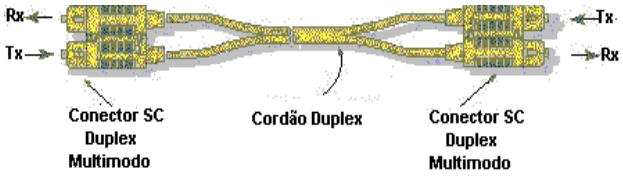


Figura 11: Polarização Inversa dos Conectores 568SC

Conclusões

Iniciou-se, com este artigo, uma discussão sobre alguns aspectos das Normas de Cabeação Estruturada EIA/TIA 568 e ISO/IEC 11801. Assim, foram apresentados um breve histórico do assunto, bem como conceitos que estão associados ao tema, além de uma análise de desempenho do hardware e dos meios de transmissão que constam na norma.

Na próxima edição deste boletim, serão vistos outros aspectos, tais como: o tratamento de código de cores para o sistema de cabeação UTP, os padrões de cabeação para redes locais de alta velocidade e a parte de gerenciamento de sistemas de cabeação estruturada.

1.4. Código de cores para sistemas de cabeação UTP

A EIA/TIA 568A define um sistema de codificação com quatro cores básicas, em combinação com o branco, para os condutores UTP de 100 Ohms, assim como a ordem dos pares no conector RJ-45, conforme ilustrado na figura 12.

a) Código de cores da cabeação UTP 100 Ohms segundo o padrão EIA/TIA 568A

PINO	CORES
1	BRANCO-VERDE
2	VERDE
3	BRANCO-LARANJA
4	AZUL
5	BRANCO-AZUL
6	LARANJA
7	BRANCO-MARROM
8	MARROM

b) Ordem dos pares no conector RJ-45 fêmea

Um outro padrão de cores da cabeação UTP, derivado da EIA/TIA 568A, o padrão EIA/TIA 568B, não muito utilizado nos dias atuais, define a seqüência de cores da Figura 13:

a) Código de cores da cabeação UTP 100 Ohms segundo o padrão EIA/TIA 568B

PINO	CORES
1	BRANCO-LARANJA
2	LARANJA
3	BRANCO-VERDE
4	AZUL
5	BRANCO-AZUL
6	VERDE
7	BRANCO-MARROM
8	MARROM

b) Ordem dos pares no conector RJ-45 fêmea

PADRÕES DE CABEAÇÃO PARA REDES LOCAIS DE ALTA VELOCIDADE

O IEEE (Institute of Electrical and Electronic Engineering) estabeleceu, recentemente, novos padrões para redes locais de alta velocidade a 100 Mbps : IEEE 802.3 100Base-T / Fast Ethernet e 802.12/ 100VGAnyLAN.

O Padrão IEEE 802.3 100Base-T é uma tecnologia de rede local de alta velocidade a 100 Mbps baseado no método de acesso CSMA/CD que inclui:

a) 100Base-TX: 2 pares de fios UTP Categoria 5 ou 2 pares tipo STP;
b) 100Base-FX: 2 fibras ópticas de 62,5/125 mm multimodo;
c) 100Base-T4: 4 pares de fios UTP categoria 3 ou 5.

O IEEE 802.12 100VGAnyLAN pode suportar, tecnicamente, distâncias maiores para os cabos UTP e STP, numa solução proprietária. Entretanto, o uso desta tecnologia para distâncias maiores que 90m, especificada pelo padrão, conduz a uma violação da norma EIA/TIA 568A.

Os padrões 100Base-TX, IEEE 802.12 100VG e EIA/TIA 568A, incluem suporte para cabos STP tipo 1A ou B de 150 Ohms, mas ninguém parece estar mais instalando-os.

O Fórum ATM publicou a especificação para suportar 155 Mbps ATM em cima do padrão EIA/TIA 568A, categoria 5-UTP. Originalmente especificado para suportar somente fibra, a interface ATM a 155 Mbps com o suporte adicional para cobre tende a reduzir significativamente os preços para o hardware ATM.

A migração de tecnologias dentro de uma corporação não é uma tarefa simples, necessitando de investimentos e, muitas vezes, de mudança na infra-estrutura básica de cabeação. Muitas empresas, hoje, ainda convivem com tecnologia de cabeação baseada em cabo coaxial. Apesar de ser uma tecnologia simples, barata e relativamente fácil de instalação e manutenção, ela torna-se um estrangulamento nas mudanças tecnológicas. Por

exemplo; o velho e ultrapassado cabo coaxial 10Base2 de 10 Mbps não suporta mais tecnologias a 100 Mbps tipo Fast Ethernet. A utilização de cabeação UTP e fibra óptica, normatizada pela EIA/TIA 568A é quase que um selo de garantia para o funcionamento adequado deste novo tipo de tecnologia de redes locais a 100 Mbps.

Apesar de sua grande importância na estruturação de sistemas de cabeação prediais para redes de 10 ou 100 Mbps, a norma EIA/TIA 568A ainda é pouco utilizada, provavelmente por falta de informações de vendedores e técnicos da área. Por exemplo, dobrar cabos e fios, apertar em demasia as cintas que agrupam um conjunto de cabos, exceder as limitações de distância, utilizar categoria de cabos inadequada para determinadas aplicações, decapar o revestimento do cabo UTP Categoria 5 mais que ½ polegada, são erros grosseiros cometidos numa instalação de cabeação, afetando variáveis de atenuação e ruído.

Figura 13: Padrão de Cores da Cabeação UTP 100W e Pinagem EIA/TIA 568B

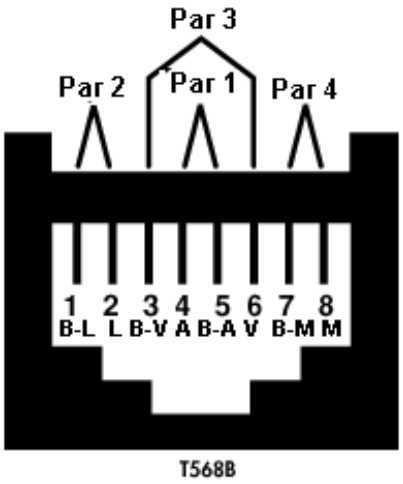
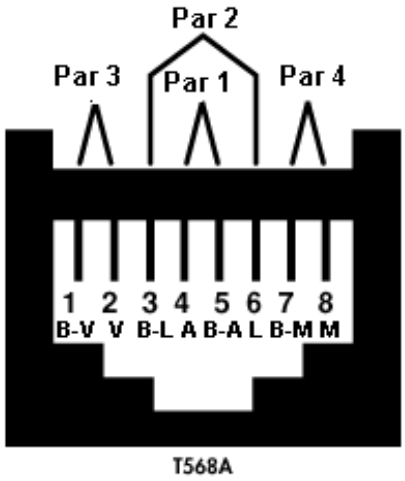


Figura 12: Padrão de Cores da Cabeação UTP 100W e Pinagem EIA/TIA 568A



^

1.5. Gerenciamento de sistemas de cabeação estruturada

Historicamente, o gerenciamento de sistemas de Cabeação Estruturada tem sempre ficado em segundo plano. Recentemente, as empresas têm reconhecido a importância da instalação de uma infra-estrutura de cabeação padronizada, além da, como consequência inevitável disso, necessidade de se estabelecer estratégias de controle eficientes para gerenciar esta mesma infra-estrutura.

Quando se parte para a escolha de uma estratégia de gerenciamento que melhor se adeque à realidade da empresa, duas questões devem ser levadas em consideração independentemente da opção escolhida: padronização e documentação.

A padronização de um sistema de cabeação, no que diz respeito aos componentes e equipamentos utilizados em toda a organização, pode prover uma economia significativa em tempo de resposta e treinamento de equipes de suporte. Em adição a um sistema de cabeação com componentes padronizados, deve existir também um sistema de numeração consistente e que seja conciso e fácil de entender.

Uma documentação precisa e compreensiva é fundamental para o sucesso de qualquer política de controle de um sistema de cabeação. Questões como planejamento de mudanças de instalações e mudanças de lay-out, aumento do número de pontos da rede, análise de falhas e uma rápida recuperação de informações devem ser consideradas como funções de uma documentação confiável. Por esses motivos, a documentação deve ser simples e confortável no uso, pois se não for dessa forma, os usuários a evitarão e o seu conteúdo se deteriorará rapidamente até o ponto em que cairá no desuso.

Existem três tipos de sistemas de gerenciamento de Cabeação Estruturada: sistemas em papel, sistemas computadorizados usando softwares de mercado e sistemas computadorizados usando softwares sob encomenda.

Sistemas em Papel

São sistemas que encontram-se em plena substituição pelos sistemas computadorizados e que propiciam a falha humana por não terem nenhum recurso que assegure que a informação é confiável e consistente. Além disso, o meio em que está armazenado é frágil e se deteriora rapidamente com o uso freqüente, podendo ocasionar a perda de informações relevantes.

Sistemas Computadorizados com Softwares de Mercado

Sistemas prontos já têm sido usados há um bom tempo para documentação de sistemas de cabeação como uma opção de substituição imediata daqueles em papel. No entanto, esta estratégia apenas resolve uma parte dos problemas provenientes dos sistemas em papel, pois continua sem nenhum tipo de validação de entrada de informação o que continua facilitando o erro humano. Esses sistemas pré-concebidos não são capazes também de simplificar e reconsiderar o esquema de numeração das organizações.

Uma evolução dos sistemas prontos são os do tipo CAD e os ditos orientados a banco de dados.

As aplicações CAD usam um desenho da estrutura do prédio como base para a documentação. Os itens no desenho têm registros em banco de dados associado a eles e um banco de dados paralelo é usado para armazenar os circuitos que resultam das conexões estabelecidas.

Já as aplicações orientadas a banco de dados têm todas as informações armazenadas de tal forma que maiores recursos de manipulação de dados e referências cruzadas possam ser utilizados. Alguns têm a capacidade de exibir a localização de uma informação a partir de uma planta baixa importada de uma aplicação CAD.

Sistemas Sob Encomenda

Nesses sistemas "customizados", é importante avaliar cuidadosamente as características de escalabilidade do software para futuras ampliações ou alterações, a estabilidade e o suporte da software house, bem como o tempo de retorno do custo do software.

Adotando-se uma estratégia de gerenciamento adequada obtém-se os seguintes benefícios:

a) Redução do tempo necessário para realizar mudanças físicas e de lay-out e ampliações na rede
b) Redução do tempo perdido na recuperação de falhas
c) Aumento do tempo de vida da infra-estrutura de cabeação.

1.6. Conclusão

A norma EIA/TIA 568A estabelece um mínimo de um cabo UTP Categoria 3 ou 5 para cada área de trabalho. Hoje em dia, levando-se em conta as tecnologias de redes locais disponíveis recomenda-se a Categoria 5.

Para o sub-sistema de Cabeação Horizontal existem duas recomendações básicas:

a) Instalar dois cabos UTP Categoria 5 de 4 pares, separados, para cada Área de Trabalho. Caso o orçamento permita, é aconselhável a instalação de dois pontos de fibra multimodo e dois ou três UTP Categoria 5.

b) Recomenda-se optar por instalar diretamente a fibra óptica, eliminando a transitoriedade da instalação da cabeação UTP Categoria 5. Esta solução traz como vantagem um tempo de vida útil maior que a com UTP Categoria 5. A cabeação com fibra óptica, entre o painel de telecomunicações e as estações de trabalho, não apresenta um custo muito significativo em relação a ao cabo UTP Categoria 5. O problema da solução com fibra óptica reside na aquisição de equipamentos com conectividade óptica: hubs, adaptadores, transceivers, etc., que atualmente são caros.

Como conclusão, para uma instalação robusta e confiável de um sistema estruturado de cabeação, recomenda-se seguir três passos básicos:

a) Instalação de fibra óptica no backbone e UTP Categoria 5, como Cabeação Horizontal, dos Armários de Telecomunicações até as Áreas de Trabalho;

b) Treinamento de funcionários ou contratação de empresas especializadas, e de boa referência, para a instalação do seu sistema;

c) Seguir a norma de instalação EIA/TIA 568A.

3 – *O Cabo Fibra Ótica*

Fibras óticas são fios finos e flexíveis de vidro ou plástico transparente que podem conduzir luz visível. Elas consistem de duas camadas concêntricas chamadas núcleo e casca. O núcleo e a casca são protegidos por uma cobertura, formando o cabo de fibra ótica. A cobertura de mais flexibilidade à fibra ótica.

As Fibras Óticas são classificadas de duas formas:

- Pelo material que elas são feitas;
- Pelo índice de refração do núcleo e o número de modos pelos quais propaga a luz na fibra.

Três combinações diferentes de materiais são usados para construir fibras óticas. Essas combinações são:

- Núcleo e casca de vidro.
- Núcleo de vidro e casca de plástico.
- Núcleo e casca de plástico.

As fibras óticas também são classificadas de acordo com seus índices de refração:

- Multi-modo degrau.
- Multi-modo gradual.
- Mono-modo.

Tipos De Fibras Ópticas

1- Vidro(Sílica)
A. Fibras monomodo índice degrau
B. Multimodo índice gradual
C. Multimodo índice degrau

2- Sílica com Casca Plástica(PCS) - Fibras de Índice Degrau

3- Plástica - Fibras Índice Degrau

Características
Fibra Monomodo

- Alcança velocidades em Gbps a uma distância de cerca de 100km.
- Empregadas em redes de longas distâncias.
- Requer fonte de laser.

Fibras Monomodo Índice Degrau

A. Aplicações para grande largura de banda (350 Ghz-1991)
B. Baixas perdas: tipicamente 0,3 dB/km até 0,5 dB/Km (1300 nm), e 0,2 dB/km (1550 nm)
C. Área do diâmetro do Campo modal de 10 mícrons
D. Diâmetro Externo de Revestimento de 125 mícron
E. Custos superiores para conectores, emendas, equipamentos de teste e transmissores/ receptores
F. Transmite um modo ou caminho de luz
G. Transmite em comprimento de onda de 1300 e 1550 nm
H . Fabricada em comprimento de até 25Km
I . Sensível a dobras (curvaturas).

Fibra Multímodo

- Não necessita uso de amplificadores.
- Tem capacidade de transmissão de ordem de 100Mbps atingindo até 2Km.
- Mais empregados em redes locais.

Fibras Multimodo Índice Gradual

A. Largura de Banda da ordem de1500 Mhz-Km
B. Perdas de 1 a 6 dB/Km
C. Núcleos de 50/ 62/ 85/ 100 mícrons (Padrões CCITT)
D. Diâmetro Externo do Revestimento de 125 e 140 mícrons
E. É eficaz com fontes de laser e LED
F. Componentes, equipamentos de teste e transmissores/ receptores de baixo custo
G. Transmite muitos modos (500+-) ou caminhos de luz, admite muitos modos de propagação
H. Possui limitação de distância devido às altas perdas e dispersão modal.
I. Transmite à 820-850 e 1300 nm.
J. Fabricadas em comprimentos até 2,2 Km

EMENDAS DE FIBRAS ÓPTICAS

Basicamente temos dois tipos de emendas utilizados na junção de cabos ópticos :

- Emenda Mecânica
- Emenda por Fusão

Emenda Mecânica : Este tipo de emenda é muito utilizado nos Estados Unidos, pela AT&T. No Brasil, encontra muita aplicação no reparo emergencial de cabos ópticos .
Consiste na utilização de conectores mecânicos , com a utilização de cola e polimento. Alguns tipos não se baseiam no polimento, devendo neste caso as fibras serem muito bem clivadas .

Emenda por fusão: este tipo de emenda é a das mais importantes e a mais utilizada atualmente. As duas extremidades a serem unidas são aquecidas até o ponto de fusão, enquanto uma pressão axial adequada é aplicada no sentido de unir as partes. Importante deixar ambas as extremidades separadas por uma distância de 10 a 15um, para permitir a dilatação do vidro.
Na prática tem-se conseguido atenuação em torno de 0.05 dB .

Conectores para FIBRA ÓTICA.
Os Concetores para a fibra ótica podem ser do tipo:

- Conector SMA.
- Conector FC-PC
- Conector D4
- Conector ST
- Conector Bicônico
- Conector SC

Os tipos padrões de fibras para redes Ethernet.

10baseFL (Fiber Link)
- taxa de transmissão de 10 Mbps
- Limites de transmissão de 2 km (Multímodo)

100baseFX
- Taxa de transmissão de 100Mbps
- Limites de transmissão de 2km (Multímodo) ou 20 km (monomodo)

1000BaseSX (Short)
- Taxa de transmissão de 1 Gbps
- Limite de transmissão de 220m (Multímodo)

1000BaseLX (Long)
- Taxa de Transmissão de 1Gbps
- Limite de transmissão de 550m (multímodo) e 5 Km (monomodo).

VANTAGENS DA FIBRA ÓPTICA

1 - Imunidade à Interferências

O feixe de luz transmitido pela fibra óptica não sofre interferência de sistemas eletromagnéticos externos.

2 - Sigilo

Devido à dificuldades de extração do sinal transmitido, obtém-se sigilo nas comunicações.

3 - Tamanho Pequeno

Um cabo de 3/8 de polegada (9,18mm) com 12 pares de fibra, operando à 140 MBPS pode carregar tantos canais de voz quanto um de 3 polegadas (73mm) de cobre com 900 pares trançados. Menor tamanho significa melhor utilização de dutos internos.

4 - Condutividade elétrica nula

A fibra óptica não precisa ser protegida de descargas elétricas, nem mesmo precisa ser aterrada, podendo suportar elevadas diferenças de potencial.

5 - Leveza

O mesmo cabo óptico citado no item 2 pesa aproximadamente 58 kg/km. O cabo de pares trançados pesa 7.250 Kg/km. Isto possibilita maiores lances de puxamento para o cabo de fibra óptica.

6 - Largura de Banda

Fibras ópticas foram testadas até os 350 bilhões de bits por segundo em uma distância de 100km. Taxas teóricas de 200-500 trilhões de bits por segundo são alcançáveis.

7 - Baixa Perda

As fibras monomodo atuais possuem perdas tão baixas quanto 0,2 dB/km (Em 1550 nm).

8 - Imunidade à Ruídos

Diferente dos sistemas metálicos, que requerem blindagem para evitar radiação e captação eletromagnética, o cabo óptico é um dielétrico e não é afetado por interferências de rádio frequência ou eletromagnéticas. O potencial para baixas taxas de erro, elevam a eficiência do circuito. As fibras ópticas são o único meio que podem transmitir através de ambientes sob severa radiação.

9 - Alta Faixa de Temperatura

Fibras e cabos podem ser fabricados para operar em temperaturas de -40º C até 93ºC. Há registros de resistência a temperatura de -73ºC até 535ºC.

10 - Sem Risco de Fogo ou Centelhamento

As fibras ópticas oferecem um meio para dados sem circulação de corrente elétrica. Para aplicações em ambientes perigosos ou explosivos, elas são uma forma de transmissão segura.

OS CONCENTRADORES

HUBS

Hubs são dispositivos utilizados para conectar os equipamentos que compõem uma rede são chamados de dispositivos concentradores pois com o Hub, as conexões da rede ficam todas em um só ponto, ficando cada equipamento com o seu cabo próprio sem interferência um com o outro.

O gerenciamento da rede é favorecido e a solução de problemas facilitada, uma vez que o defeito fica isolado no segmento de rede. Cada hub pode receber vários micros, atualmente temos hub's com 4,8,16 e 32 portas. Os HUBs necessitam apenas de ser alimentados para funcionar, não necessita de software para que cumpram sua finalidade em uma rede, na verdade os PCs envolvidos na comunicação entre eles não reconhecem ou enxergam o HUB, devido a isto podemos desconectar qualquer PC de um HUB sem causar nenhum problema de funcionamento do sistema operacional, o que acontecerá será apenas que o PC deixara de se comunicar com a rede, e ao religarmos o cabo tudo se normalizará.

Normalmente é indicado pelos fabricantes dos HUBs que a distancia entre o PC e HUB não seja maior que 100 metros, mas pode-se exceder esta distância para até 150 metros que normalmente não causará problema nenhum, lógico que deverá ser observado alguns fatores assim como:

- As conexões sejam bem feitas.
- O cabo par trançado seja de boa qualidade.
- Não haja interferência eletromagnética (o cabo não pode trafegar junto ou próximo à fiação elétrica).
- No lançamento dos cabos ele nunca deve ser tracionado, pois perderá suas características elétricas.

É possível interligar vários Hubs (cascateamento), se por exemplo têm-se dois Hubs de oito portas e há a necessidade de interligar doze máquinas faz-se o seguinte.

Colocam-se seis cabos em cada Hub e conecta-se outro cabo interligando os dois Hubs, sendo que o comprimento do cabo de interligação não deve ser menor que 0,5 metros ou maior que cinco metros (especificação da maioria dos fabricantes).

Alguns Hubs já vem com uma porta especial (porta UpLink) está porta é igual as demais com a diferença de não ter os sinais de transmissão e recepção cruzados como as outras e uns tem até uma pequena chave ao lado da saída UpLink para se ativar ou desativar o cruzamento dos sinais mas se no seu HUB não houver a saída UpLink devemos confeccionar o cabo Cross-Over como o que usamos para interligar dois computadores.

Na verdade é sempre bom obter informação no catálogo técnico do equipamento ou no site do fabricante para se evitar perda de tempo ou até perda do próprio equipamento ou no site do fabricante para se evitar perda de tempo ou até perda do próprio equipamento.

SWITCH

Os Switchs funcionam diferentemente dos HUBs pois não compartilham barramento onde os quadros são transmitidos simultaneamente para todas as portas (broadcast), oferecem uma linha comutada dedicada a cada uma das suas conexões, o switch permitiria que cada conexão se comunicasse à velocidade total da LAN. Com isso os switch permitem comunicações paralelas, onde duas estações podem enviar seus dados em um mesmo intervalo de tempo sem riscos de colisões.

REPETIDOR (REPEATER)

O repetidor é um dispositivo responsável por ampliar o tamanho Maximo do cabeamento da rede. Ele funciona como um amplificador de sinais, regenerando os sinais recebidos e transmitindo esses sinais para outro segmento da rede.

PONTE (BRIDGE)

A ponte é um repetidor inteligente. É um equipamento que segmenta a rede em duas partes, geralmente colocada entre dois Hub's, no sentido de melhorar a segurança ou o trafego de rede. A ponte atua na camada de Link de Dados (Enlace) conforme o modelo OSI, ou seja, a ponte atua na leitura e interpretação dos quadros (frames) de dados da rede, bem diferente de hubs e repetidores que atuam na camada física manipulando sinais elétricos.

ROTEADORES

Um roteador é um dispositivo que provê a comunicação entre duas ou mais LAN's, gerencia o tráfego de uma rede local e controla o acesso aos seus dados, de acordo com as determinações do administrador da rede. O roteador pode ser uma máquina dedicada, sendo um equipamento de rede específico para funções de roteamento; ou pode ser também um software instalado em um computador.
Consideremos por exemplo um grupo de dispositivos de rede, como servidores, PC's e impressoras, formando uma rede local a qual chamamos de LAN 1, como mostrado na figura abaixo. Consideremos também outra rede local, similar a primeira, a qual chamamos de LAN 2. A interconexão entre elas, que permite a troca de dados e o compartilhamento dos seus recursos e serviços, é feita pelo roteador. Esse esquema caracteriza o uso de uma máquina dedicada.

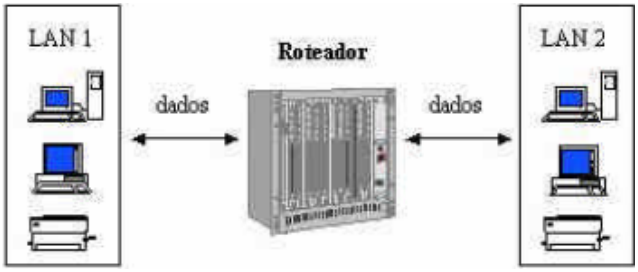


Figura: O roteador permite o tráfego de informações e o compartilhamento de serviços e recursos entre redes diferentes.

Consideremos agora a figura mostrada a seguir. Nela está representado o caso em que o roteador é um software instalado em um computador. Como podemos observar, é o computador, através de um software específico, que gerencia o tráfego de dados entres as diferentes redes mostradas. Esse esquema representa a topologia de rede inicialmente utilizada no CBPF até 1996, quando um servidor Novell exercia a função de um roteador, através de um software de roteamento fabricado pela própria Novell.
O roteador opera na camada de rede, a terceira das sete camadas do modelo de referência ISO OSI. Esse modelo de rede foi criado pela ISO (International Organization of Standardization) no início dos anos oitenta, tendo sido o primeiro passo para a padronização internacional dos diversos protocolos de comunicação existentes atualmente. Quanto ao funcionamento de um roteador, tem-se que quando pacotes (partes da mensagem que é transmitida) são transmitidos de um host (qualquer dispositivo de uma rede) para outro, esses equipamentos usam cabeçalhos (headers) e uma tabela de roteamento para determinar por qual caminho esses pacotes irão; os roteadores também usam o protocolo ICMP (Internet Control Message Protocol) para comunicarem-se entre si e configurarem a melhor rota entre dois hosts quaisquer. O cabeçalho, em várias disciplinas da ciência da computação, é definido como uma unidade de informação que antecede o objeto de dados de um pacote; ou seja, é no cabeçalho que está contida a informação sobre o destino do pacote utilizada pelo roteador. Já em relação ao ICMP, temos que ele é uma extensão do protocolo IP (Internet Protocol), sendo definido pela RFC 792. O ICMP suporta pacotes que contenham mensagens de erro, de controle e de informação. O comando ping, por exemplo, usa esse protocolo para testar uma conexão Internet.

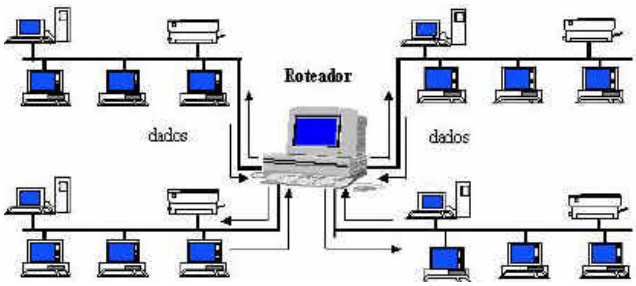


Figura : Um computador, através de software específico, pode gerenciar o tráfego de dados entre redes diferentes, funcionando como um roteador.

Por último, temos que uma pequena filtragem de dados é feita através de roteadores. Contudo, é importante ressaltar que os roteadores não se preocupam com o conteúdo dos pacotes com que eles lidam, verificando apenas o cabeçalho de cada mensagem, podendo ou não tratá-la de forma diferenciada.

Resumo das características do Roteador

- é um dispositivo que serve para interligar diferentes redes.
- trabalha na camada de Rede do modelo OSI.
- entende a informação como datragramas, ou seja, consegue ler o endereço IP do pacote.

- trabalha com a troca de tabelas de roteamento.
- trabalha com protocolos de roteamento (menor caminho ou melhor caminho).

Os protocolos de Roteamento do Roteador

Protocolo baseado no caminho mais curto:

- RIP (Routing Information Protocol – usado pelo IP e pelo IPX)
- RTMP (usado pelo Apple Talk),

Protocolo baseado no melhor caminho:

- OSPF (usado pelo IP),
- NLSP (usado pelo IPX)
- PNNI (usado pelo ATM)

A Internet

A WWW (World Wide Web)

A World Wide Web é a estrutura pela qual conseguimos acessar documentos espalhados por todo mundo na internet. Em seus primórdios, os documentos eram formados somente de texto, mas com o tempo foram-se agregando figuras (jpeg, gif, etc), animações gráficas (flash, gifs animados, etc), áudio (au, wav, MP3), vídeos (MPEG, divx), desta maneira, os documentos tornaram-se mais poderosos e a interface mais amigável, repercutindo em sua enorme popularidade atual. A WWW, que também é conhecida como *Web*, e por isso do nome servidor *Web*.

A principal função do servidor web é disponibilizar dados, podendo ser imagens, vídeo, áudio ou arquivos em geral. Estes dados são passados para os *clientes* para que possam exibir as informações. O cliente de um servidor web é o browser ou navegador (Internet Explorer, Netscape Navigator, Opera, Lynx, Mozila Firefox) e o formato entendido por estes é o HTML – linguagem utilizada para formatar e definir páginas da internet. É assim que a internet funciona através de uma estrutura chamada de ***cliente/servidor***. Onde cliente é aquele que solicita uma ação e servidor é o agente que reponde a solicitação de um cliente.

O servidor web utiliza-se do protocolo http, o protocolo mais conhecido da Internet, que usa de hipertextos, que são textos com referências (links) que levam a outros textos, formando uma teia (web) da páginas interligadas, daí vem o nome WWW que significa *Grande Teia Mundial* ou *Rede Mundial de Computadores*.

O acesso à internet passa por duas etapas: **a conexão** e **a navegação.**

A Conexão

A conexão é o primeiro passo para o usuário que queira acessar a internet, o acesso deve ser feito através de um computador que forneça esse acesso o *servidor web* também conhecido como *provedor de acesso*.

Os tipos de acesso à internet podem ser:

Provedores comerciais – IG, BOL, UOL, TERRA, etc.

Provedores públicos – órgãos do governo federal ou estadual (secretarias, ministérios, universidades, forças armadas, etc).

On-line – são as empresas que provém o acesso direto à internet (EMBRATEL, GVT, BRASILTELECOM).

A navegaçao é feita utilizando-se os programas de navegação também chamados de *browsers.*

Redes Wireless (sem fio)

As redes sem fio são divididas em várias partes, as duas que mais são discutidas em provas são ***WLAN (Wireless LAN)*** que são as redes sem fio de pequeno alcance, ou seja, redes locais sem fio ***e WWAN (Wireless WAN)*** que são as redes sem fio empregadas nas redes remotas, ou seja, nas redes geograficamente distribuídas.
Segue abaixo alguns exemplos de redes **WLAN e WWAN:**

WLAN (Wireless Local Area Network)

Os principais padrões de redes de pequeno alcance (WLAN) são conhecidos como:

- **BLUETOOTH** – Usado para a interconectar dispositivos de computação e comunicação e ainda acessórios, utilizando rádios sem fio de curto alcance, baixa potência e baixo custo. A unidade básica dentro de uma rede *Bluetooth* é o *piconet* o o sistema utiliza uma freqüência de até 2,4 GHz, com uma taxa de transmissão de aproximadamente 1 Mbps, com distância máxima de 10 metros.
- **Wi-Fi** - O termo wi-fi é a abreviatura de *wireless fidelity* e que pode ser traduzido como "fidelidade sem fios". Muito utilizada para promover acesso em banda larga à Internet em locais públicos, tais como hotéis, aeroportos e centros de convenções de maneira rápida, fácil e sem a necessidade de cabos. O acesso a Internet no wi-fi ocorre através de um *hostpost* que é um ponto de acesso (*access point)* colocado em um local público e o alcance produzido chega a 350 metros.
- **Infravermelho** - A utilização do infravermelho para a comunicação sem fio tem sua aplicação voltada mais para redes locais. Seu alcance está restrito a um ambiente pequeno e totalmente sem obstáculos, pois o espectro de luz não pode atravessá-los. Usada principalmente para conectar teclado, mouse, controle de vídeo game, etc.

O que são Redes Wireless?

A palavra wireless provém do inglês: wire (fio, cabo); less (sem); ou seja: sem fios. Wireless então caracteriza qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos. Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar. Pela extrema facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Dentro deste modelo de comunicação, enquadram-se várias tecnologias, como Wi-Fi, InfraRed (infravermelho), bluetooth e Wi-Max.

Seu controle remoto de televisão ou aparelho de som, seu telefone celular e uma infinidade de aparelhos trabalham

com conexões wireless. Podemos dizer, como exemplo lúdico, que durante uma conversa entre duas pessoas, temos uma conexão wireless, partindo do principio de que sua voz não utiliza cabos para chegar até o receptor da mensagem.

Nesta categoria de redes, há vários tipos de redes que são: Redes Locais sem Fio ou WLAN (Wireless Local Area Network), Redes Metropolitanas sem Fio ou WMAN (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou WWAN (Wireless Wide Area Network), redes WLL (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (Wireless Personal Area Network).

As aplicações de rede estão dividas em dois tipos: aplicações indoor e aplicações outdoor. Basicamente, se a rede necessita de comunicação entre dois ambientes, a comunicação é realizada por uma aplicação outdoor (dois prédios de uma mesma empresa, por exemplo). A comunicação dentro de cada um dos prédios é caracterizada como indoor. A comunicação entre os dois prédios é realizada por uma aplicação outdoor.

Como funcionam?

Através da utilização portadoras de rádio ou infravermelho, as WLANs estabelecem a comunicação de dados entre os pontos da rede. Os dados são modulados na portadora de rádio e transmitidos através de ondas eletromagnéticas.

Múltiplas portadoras de rádio podem coexistir num mesmo meio, sem que uma interfira na outra. Para extrair os dados, o receptor sintoniza numa freqüência específica e rejeita as outras portadoras de freqüências diferentes.

Num ambiente típico, o dispositivo transceptor (transmissor/receptor) ou ponto de acesso (access point) é conectado a uma rede local Ethernet convencional (com fio). Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os pontos de acesso vizinhos, num esquema de micro células com roaming semelhante a um sistema de telefonia celular.

A topologia da rede é composta de que?

- BSS (Basic Service Set) - Corresponde a uma célula de comunicação da rede sem fio.
- STA (Wireless LAN Stations) - São os diversos clientes da rede.
- AP (Access Point) - É o nó que coordena a comunicação entre as STAs dentro da BSS. Funciona como uma ponte de comunicação entre a rede sem fio e a rede convencional.
- DS (Distribution System) - Corresponde ao backbone da WLAN, realizando a comunicação entre os APs.
- ESS (Extended Service Set) - Conjunto de células BSS cujos APs estão conectados a uma mesma rede convencional. Nestas condições uma STA pode se movimentar de uma célula BSS para outra permanecendo conectada à rede. Este processo é denominado de Roaming.

< modos dois de configuradas ser podem WLANs redes>

As Redes WLAN Podem ser configuradas como:

- Ad-hoc mode – Independent Basic Service Set (IBSS)

A comunicação entre as estações de trabalho é estabelecida diretamente, sem a necessidade de um AP e de uma rede física para conectar as estações.

- Infrastructure mode – Infrastructure Basic Service Set

A rede possui pontos de acessos (AP) fixos que conectam a rede sem fio à rede convencional e estabelecem a comunicação entre os diversos clientes.

Tecnologias empregadas

Há várias tecnologias envolvidas nas redes locais sem fio e cada uma tem suas particularidades, suas limitações e suas vantagens. A seguir, são apresentadas algumas das mais empregadas.

- Sistemas Narrowband: Os sistemas narrowband (banda estreita) operam numa freqüência de rádio específica, mantendo o sinal de de rádio o mais estreito possível o suficiente para passar as informações. O crosstalk indesejável entre os vários canais de comunicação pode ser evitado coordenando cuidadosamente os diferentes usuários nos diferentes canais de freqüência.

- Spread Spectrum: É uma técnica de rádio freqüência desenvolvida pelo exército e utilizado em sistemas de comunicação de missão crítica, garantindo segurança e rentabilidade. O Spread Spectrum é o mais utilizado atualmente. Utiliza a técnica de espalhamento espectral com sinais de rádio freqüência de banda larga, foi desenvolvida para dar segurança, integridade e confiabilidade deixando de lado a eficiência no uso da largura de banda. Em outras palavras, maior largura de banda é consumida que no caso de transmissão narrowaband, mas deixar de lado este aspecto produz um sinal que é, com efeito, muito mais ruidoso e assim mais fácil de detectar, proporcionando aos receptores conhecer os parâmetros do sinal spread-spectrum via broadcast. Se um receptor não é sintonizado na freqüência correta, um sinal spread-spectrum inspeciona o ruído de fundo. Existem duas

alternativas principais: Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS).

Direct Sequence Spread Spectrum (DSSS): Gera um bit-code (também chamado de chip ou chipping code) redundante para cada bit transmitido. Quanto maior o chip maior será a probabilidade de recuperação da informação original. Contudo, uma maior banda é requerida. Mesmo que um ou mais bits no chip sejam danificados durante a transmissão, técnicas estatísticas embutidas no rádio são capazes de recuperar os dados originais sem a necessidade de retransmissão. A maioria dos fabricantes de produtos para Wireless LAN tem adotado a tecnologia DSSS depois de considerar os benefícios versus os custos e benefício que se obtém com ela. Tal é o caso dos produtos Wireless da D-Link.

Frequency-hopping spread-spectrum (FHSS): Utiliza um sinal portador que troca de freqüência no padrão que é conhecido pelo transmissor e receptor. Devidamente sincronizada, a rede efetua esta troca para manter um único canal analógico de operação.

Outras Tecnologias

A comunicação wireless está presente há um bom tempo no nosso cotidiano. Falemos da conexão sem fio mais comum – os controles remotos para televisores, som, DVD, entre outros, utilizam conexão por raios infravermelhos (InfraRed). Essa conexão atua em um alcance máximo de 5m aproximadamente, e com ângulo de 45 graus a partir da fonte.

Apesar de oferecer conexão, o InfraRed trazia a inconveniência de sempre necessitar do alinhamento dos dispositivos, o que criava uma certa dificuldade para locomoção, além de ter a mesma velocidade de uma porta serial. Foi então desenvolvida a tecnologia conhecida como bluetooth. Essa tecnologia atua em um raio de 10m, com uma velocidade maior que o InfraRed, utilizando a Rádio Freqüência.
Com bluetooth, o sinal se propaga em todas as direções, não necessita alinhamento e torna a locomoção mais fácil. Os padrões de velocidade são:

- Assíncrono, a uma taxa máxima de 723,2 kbit/s (unidirecional).
- Bidirecional síncrono, com taxa de 64 kbit/s, que suporta tráfego de voz entre os dois dispositivos.

Com o sucesso do Wi-Fi, a Intel começou a apoiar uma outra nova tecnologia denominada Wi-Max. Esta conexão wireless de alta velocidade permite um alcance de até cerca de 48 quilômetros.
Uma outra solução é a Mobile-Fi, uma tecnologia que permite banda larga sem fio em veículos em movimento. A NTT DoCoMo e alguns startups trabalham atualmente na definição de um protocolo, o que deve acontecer em 2005 ou 2006. A Nextel também está conduzindo testes com o Mobile-Fi.
Uma outra tecnologia nova que desponta é a UltraWideband, que permite a transmissão de arquivos enormes sobre distâncias curtas – mesmo através de paredes. Existe no momento uma disputa pela definição deste protocolo entre Texas Instruments e Intel de um lado, e Motorola do outro.

Segurança

As principais dicas para se ter uma rede Wireless Segura

Uma rede sem fio é um conjunto de sistemas conectados por tecnologia de rádio através do ar, Com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que qualquer um possa se conectar a ela e roubar seus dados? Um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões da sua casa consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as redes sem fio vêm ganhando. Para garantir a segurança, existem vários sistemas que podem ser implementados, apesar de nem sempre eles virem ativados por default nos pontos de acesso.

O que realmente precisamos saber para que a rede sem fio implementada esteja com o nível correto de segurança? Em primeiro lugar é preciso conhecer os padrões disponíveis, o que eles podem oferecer e então, de acordo com sua aplicação, política de segurança e objetivo, implementar o nível correto e desejado. Ser o último disponível não garante, dependendo de sua configuração, que a segurança será eficiente. É preciso entender, avaliar bem as alternativas e então decidir-se de acordo com sua experiência e as características disponíveis nos produtos que vai utilizar, objetivando também o melhor custo.

A segurança wireless é um trabalho em andamento, com padrões em evolução. Com tempo e acesso suficientes, um hacker persistente provavelmente conseguirá invadir seu sistema wireless. Ainda assim, você pode tomar algumas atitudes para dificultar ao máximo possível o trabalho do intruso. , nas variantes de conotação maléfica da palavra. Temos, assim, práticas típicas concernentes a redes sem fio, sejam estas comerciais ou não, conhecidas como wardriving e warchalking.

Wardriving

O termo wardriving foi escolhido por Peter Shipley (http://www.dis.org/shipley/) para batizar a atividade de dirigir um automóvel à procura de redes sem fio abertas, passíveis de invasão. Para efetuar a prática do wardriving, são necessários um automóvel, um computador, uma placa Ethernet configurada no modo "promíscuo" (o dispositivo efetua a interceptação e leitura dos pacotes de comunicação de maneira completa), e um tipo de antena, que pode ser posicionada dentro ou fora do veículo (uma lata de famosa marca de batatas fritas norte-americana costuma ser utilizada para a construção de antenas) . Tal

atividade não é danosa em si, pois alguns se contentam em encontrar a rede wireless desprotegida, enquanto outros efetuam login e uso destas redes, o que já ultrapassa o escopo da atividade. Tivemos notícia, no ano passado, da verificação de desproteção de uma rede wireless pertencente a um banco internacional na zona Sul de São Paulo mediante wardriving, entre outros casos semelhantes. Os aficionados em wardriving consideram a atividade totalmente legítima.

Warchalking

Inspirado em prática surgida na Grande Depressão norte-americana, quando andarilhos desempregados (conhecidos como "hobos") criaram uma linguagem de marcas de giz ou carvão em cercas, calçadas e paredes, indicando assim uns aos outros o que esperar de determinados lugares, casas ou instituições onde poderiam conseguir comida e abrigo temporário, o warchalking é a prática de escrever símbolos indicando a existência de redes wireless e informando sobre suas configurações. As marcas usualmente feitas em giz em calçadas indicam a posição de redes sem fio, facilitando a localização para uso de conexões alheias pelos simpatizantes da idéia.

O padrão IEEE 802.11 fornece o serviço de segurança dos dados através de dois métodos: autenticação e criptografia. Este padrão 802.11 define duas formas de autenticação: **open system** e **shared key**. Independente da forma escolhida, qualquer autenticação deve ser realizada entre pares de estações, jamais havendo comunicação multicast. Em sistemas BSS as estações devem se autenticar e realizar a troca de informações através do Access Point (AP). As formas de autenticação previstas definem:

- Autenticação Open System - é o sistema de autenticação padrão. Neste sistema, qualquer estação será aceita na rede, bastando requisitar uma autorização. É o sistema de autenticação nulo.
- **Autenticação Shared key** – neste sistema de autenticação, ambas as estações (requisitante e autenticadora) devem compartilhar uma chave secreta. A forma de obtenção desta chave não é especificada no padrão, ficando a cargo dos fabricantes a criação deste mecanismo. A troca de informações durante o funcionamento normal da rede é realizada através da utilização do protocolo WEP.

A autenticação do tipo Open System foi desenvolvida focando redes que não precisam de segurança para autenticidade de dispositivos. Nenhuma informação sigilosa deve trafegar nestas redes já que não existe qualquer proteção. Também se aconselha que estas redes permaneçam separadas da rede interna por um firewall (a semelhança de uma zona desmilitarizada – DMZ).

A autenticação Shared Key utiliza mecanismos de criptografia para realizar a autenticação dos dispositivos. Um segredo é utilizado como semente para o algoritmo de criptografia do WEP na cifragem dos quadros. A forma de obter esta autenticação é a seguinte:

1. Estação que deseja autenticar-se na rede envia uma requisição de autenticação para o AP.
2. O AP responde a esta requisição com um texto desafio contendo 128 bytes de informações pseudorandômicas.
3.A estação requisitante deve então provar que conhece o segredo compartilhado, utilizando-o para cifrar os 128 bytes enviados pelo AP e devolvendo estes dados ao AP.
4.O AP conhece o segredo, então compara o texto originalmente enviado com a resposta da estação. Se a cifragem da estação foi realizada com o segredo correto, então esta estação pode acessar a rede.

Dentro do utilitário de configuração você poderá habilitar os recursos de segurança. Na maioria dos casos todos os recursos abaixo vêm desativados por default a fim de que a rede funcione imediatamente, mesmo antes de qualquer coisa ser configurada. Para os fabricantes, quanto mais simples for a instalação da rede, melhor, pois haverá um número menor de usuários insatisfeitos por não conseguir fazer a coisa funcionar. Mas, você não é qualquer um. Vamos então às configurações:

SSID

A primeira linha de defesa é o SSID (Service Set ID), um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede. Cada fabricante utiliza um valor default para esta opção, mas você deve alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar.

Geralmente estará disponível no utilitário de configuração do ponto de acesso a opção "broadcast SSID". Ao ativar esta opção o ponto de acesso envia periodicamente o código SSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber previamente o código. Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais "plug-and-play". Você não precisará mais configurar manualmente o código SSID em todos os micros.

Esta é uma opção desejável em redes de acesso público, como muitas redes implantadas em escolas, aeroportos, etc., mas caso a sua preocupação maior seja a segurança, o melhor é desativar a opção. Desta forma, apenas quem souber o valor ESSID poderá acessar a rede.

WEP

O Wired Equivalency Privacy (WEP) é o método criptográfico usado nas redes wireless 802.11. O WEP opera na camada de enlace de dados (data-link layer) e fornece criptografia entre o cliente e o Access Point. O WEP é baseado no método criptográfico RC4 da RSA, que usa um vetor de inicialização (IV) de 24 bits e uma chave secreta compartilhada (secret shared key) de 40 ou 104 bits. O IV é concatenado com a secret shared key para

formar uma chave de 64 ou 128 bits que é usada para criptografar os dados. Além disso, o WEP utiliza CRC-32 para calcular o checksum da mensagem, que é incluso no pacote, para garantir a integridade dos dados. O receptor então recalcula o checksum para garantir que a mensagem não foi alterada.

Apenas o SSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast SSID esteja desativada, já existem sniffers que podem descobrir rapidamente o SSID da rede monitorando o tráfego de dados. Eis que surge o WEP, abreviação de Wired-Equivalent Privacy, que como o nome sugere traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o SSID sozinho.

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede.

Na verdade, o WEP é composto de duas chaves distintas, de 40 e 24 bits no padrão de 64 bits e de 104 e 24 bits no padrão de 128. Por isso, a complexidade encriptação usada nos dois padrões não é a mesma que seria em padrões de 64 e 128 de verdade. Além do detalhe do número de bits nas chaves de encriptação, o WEP possui outras vulnerabilidades. Alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Como disse, o WEP não é perfeito, mas já garante um nível básico de proteção. Esta é uma chave que foi amplamente utilizada, e ainda é, mas que possui falhas conhecidas e facilmente exploradas por softwares como AirSnort ou WEPCrack. Em resumo o problema consiste na forma com que se trata a chave e como ela é "empacotada" ao ser agregada ao pacote de dados.

O WEP vem desativado na grande maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que você precisará definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço ESSID e outras configurações de rede podem ser definidos através de outro utilitário, fornecido pelo fabricante da placa.

WPA, um WEP melhorado

Também chamado de WEP2, ou TKIP (Temporal Key Integrity Protocol), essa primeira versão do WPA (Wi-Fi Protected Access) surgiu de um esforço conjunto de membros da Wi-Fi Aliança e de membros do IEEE, empenhados em aumentar o nível de segurança das redes sem fio ainda no ano de 2003, combatendo algumas das vulnerabilidades do WEP.

A partir desse esforço, pretende-se colocar no mercado brevemente produtos que utilizam WPA, que apesar de não ser um padrão IEEE 802.11 ainda, é baseado neste padrão e tem algumas características que fazem dele uma ótima opção para quem precisa de segurança rapidamente: Pode-se utilizar WPA numa rede híbrida que tenha WEP instalado. Migrar para WPA requer somente atualização de software. WPA é desenhado para ser compatível com o próximo padrão IEEE 802.11i.

Vantagens do WPA sobre o WEP

Com a substituição do WEP pelo WPA, temos como vantagem melhorar a criptografia dos dados ao utilizar um protocolo de chave temporária (TKIP) que possibilita a criação de chaves por pacotes, além de possuir função detectora de erros chamada Michael, um vetor de inicialização de 48 bits, ao invés de 24 como no WEP e um mecanismo de distribuição de chaves.

Além disso, uma outra vantagem é a melhoria no processo de autenticação de usuários. Essa autenticação se utiliza do 802.11x e do EAP (Extensible Authentication Protocol), que através de um servidor de autenticação central faz a autenticação de cada usuário antes deste ter acesso a rede.

RADIUS

Este é um padrão de encriptação proprietário que utiliza chaves de encriptação de 128 bits reais, o que o torna muito mais seguro que o WEP. Infelizmente este padrão é suportado apenas por alguns produtos. Se estiver interessado nesta camada extra de proteção, você precisará pesquisar quais modelos suportam o padrão e selecionar suas placas e pontos de acesso dentro desse círculo restrito. Os componentes geralmente serão um pouco mais caro, já que você estará pagando também pela camada extra de encriptação.

Permissões de acesso

Além da encriptação você pode considerar implantar também um sistema de segurança baseado em permissões de acesso. O Windows 95/98/ME permite colocar senhas nos compartilhamentos, enquanto o Windows NT, 2000 Server, já permitem uma segurança mais refinada, baseada em permissões de acesso por endereço IP, por usuário, por grupo, etc. Usando estes recursos, mesmo que alguém consiga penetrar na sua rede, ainda terá que quebrar a segurança do sistema operacional para conseguir chegar aos seus arquivos. Isso vale não apenas para redes sem fio, mas também para redes cabeadas, onde qualquer um que tenha acesso a um dos cabos ou a um PC conectado à rede

é um invasor em potencial. Alguns pontos de acesso oferecem a possibilidade de estabelecer uma lista com as placas que têm permissão para utilizar a rede e rejeitar qualquer tentativa de conexão de placas não autorizadas. O controle é feito através dos endereços MAC das placas, que precisam ser incluídos um a um na lista de permissões, através do utilitário do ponto de acesso. Muitos oferecem ainda a possibilidade de estabelecer senhas de acesso.

Somando o uso de todos os recursos acima, a rede sem fio pode tornar-se até mais segura do que uma rede cabeada, embora implantar tantas camadas de proteção torne a implantação da rede muito mais trabalhosa.

ACL (Access Control List)

Esta é uma prática herdada das redes cabeadas e dos administradores de redes que gostam de manter controle sobre que equipamentos acessam sua rede. O controle consiste em uma lista de endereços MAC (físico) dos adaptadores de rede que se deseja permitir a entrada na rede wireless. Seu uso é bem simples e apesar de técnicas de MAC Spoofing serem hoje bastante conhecidas é algo que agrega boa segurança e pode ser usado em conjunto com qualquer outro padrão, como WEP, WPA etc. A lista pode ficar no ponto de acesso ou em um PC ou equipamento de rede cabeada, e a cada novo cliente que tenta se conectar seu endereço MAC é validado e comparado aos valores da lista. Caso ele exista nesta lista, o acesso é liberado.

Para que o invasor possa se conectar e se fazer passar por um cliente válido ele precisa descobrir o MAC utilizado. Como disse, descobrir isso pode ser relativamente fácil para um hacker experiente que utilize um analisador de protocolo (Ethereal, por exemplo) e um software de mudança de MAC (MACShift por exemplo). De novo, para aplicações onde é possível agregar mais esta camada, vale a pena pensar e investir em sua implementação, já que o custo é praticamente zero. O endereço MAC, em geral, está impresso em uma etiqueta fixada a uma placa de rede ou na parte de baixo de um notebook. Para descobrir o endereço MAC do seu computador no Windows XP, abra uma caixa de comando (Iniciar/Todos os Programas/Acessórios/Prompt de Comando), digite **getmac** e pressione a tecla Enter. Faça isso para cada computador na rede e entre com a informação na lista do seu roteador.

Protocolos

Porquê a Necessidade de Padrões para uma LAN Sem Fios

Antes da adesão do protocolo 802.11, vendedores de redes de dados sem fios faziam equipamentos que eram baseados em tecnologia proprietária. Sabendo que iam ficar presos ao comprar do mesmo fabricante, os clientes potenciais de redes sem fios viraram para tecnologias mais viradas a protocolos.Em resultado disto, desenvolvimento de redes sem fios não existia em larga escala, e era considerado um luxo só estando ao alcance de grandes companhias com grandes orçamentos.O único caminho para redes LAN sem fios (WLAN - Wireless Local Area Network) ser geralmente aceite era se o hardware envolvido era de baixo custo e compatível com os restantes equipamentos.

Reconhecendo que o único caminho para isto acontecer era se existisse um protocolo de redes de dados sem fios. O grupo 802 do Instituto de Engenheiros da Eletrônica e Eletricidade (IEEE -Institute of Electrical and Electronics Engineers, uma associação sem fins lucrativos que reúne aproximadamente 380.000 membros, em 150 países. Composto de engenheiros das áreas de telecomunicações, computação, eletrônica e ciências aeroespaciais, entre outras, o IEEE definiu algo em torno de 900 padrões tecnológicos ativos e utilizados pela indústria, e conta com mais 700 em desenvolvimento), tomou o seu décimo primeiro desafio. Porque uma grande parte dos membros do grupo 802.11 era constituído de empregados dos fabricantes de tecnologias sem fios, existiam muitos empurrões para incluir certas funções na especificação final. Isto, no entanto atrasou o progresso da finalização do protocolo 802.11, mas também forneceu um protocolo rico em atributos ficando aberto para futuras expansões.No dia 26 de Junho em 1997, o IEEE anunciou a retificação do protocolo 802.11 para WLAN. Desde dessa altura, custo associado a desenvolvimento de uma rede baseada no protocolo 802.11 tem descido.

Desde o primeiro protocolo 802.11 ser aprovado em 1997, ainda houve várias tentativas em melhorar o protocolo.Na introdução dos protocolos, primeiro veio o 802.11, sendo seguido pelo 802.11b. A seguir veio 802.11a, que fornece até cinco vezes a capacidade de largura de banda do 802.11b. Agora com a grande procura de serviços de multimídia, vem o desenvolvimento do 802.11e. A seguir será explicado cada protocolo falando entre outros. Cada grupo, que segue tem como objetivo acelerar o protocolo 802.11, tornando-o globalmente acessível, não sendo necessário reinventar a camada física (MAC - Media Access Control) do 802.11.

802.11b

A camada física do 802.11b utiliza espalhamento espectral por seqüência direta (DSSS – Direct Sequence Spread Spectrum) que usa transmissão aberta (broadcast) de rádio e opera na freqüência de 2.4000 a 2.4835GHz no total de 14 canais com uma capacidade de transferência de 11 Mbps, em ambientes abertos (~ 450 metros) ou fechados (~ 50 metros). Esta taxa pode ser reduzida a 5.5 Mbps ou até menos, dependendo das condições do ambiente no qual as ondas estão se propagando (paredes, interferências, etc).

Dentro do conceito de WLAN (Wireless Local Area Network) temos o conhecido Wi-Fi. O Wi-Fi nada mais é do que um nome comercial para um padrão de rede wireless chamado de 802.11b, utilizado em aplicações indoor. Hoje em dia existem vários dispositivos a competir para o espaço aéreo no espectro de 2.4GHz. Infelizmente a

maior parte que causam interferências são comuns em cada lar, como por exemplo, o microondas e os telefones sem fios. Uma das mais recentes aquisições do 802.11b é do novo protocolo Bluetooth, desenhado para transmissões de curtas distâncias. Os dispositivos Bluetooth utilizam espalhamento espectral por salto na freqüência (FHSS – Frequency Hopping Spread Spectrum) para comunicar entre eles.

A topologia das redes 802.11b é semelhante a das redes de par trançado, com um Hub central. A diferença no caso é que simplesmente não existem os fios e que o equipamento central é chamado Access Point cuja função não defere muito da hub: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam, existem tanto placas PC-Card, que podem ser utilizadas em notebooks e em alguns handhelds, e para placas de micros de mesa.

Exemplo de uma rede 802.11b

802.11g

Este é o irmão mais novo do 802.11b e que traz, de uma forma simples e direta, uma única diferença: Sua velocidade alcança 54 Mbits/s contra os 11 Mbits/s do 802.11b. Não vamos entrar na matemática da largura efetiva de banda dessas tecnologias, mas em resumo temos uma velocidade três ou quatro vezes maior num mesmo raio de alcance. A freqüência e número de canais são exatamente iguais aos do 802.11b, ou seja, 2.4GHz com 11 canais (3 non overlaping).

Não há muito que falar em termos de 802.11g senão que sua tecnologia mantém total compatibilidade com dispositivos 802.11b e que tudo o que é suportado hoje em segurança também pode ser aplicado a este padrão. Exemplificando, se temos um ponto de acesso 802.11g e temos dois laptops conectados a ele, sendo um 802.11b e outro 802.11g, a velocidade da rede será 11 Mbits/s obrigatoriamente. O ponto de acesso irá utilizar a menor velocidade como regra para manter a compatibilidade entre todos os dispositivos conectados.

No mais, o 802.11g traz com suporte nativo o padrão WPA de segurança, que também hoje já se encontra implementado em alguns produtos 802.11b, porém não sendo regra. O alcance e aplicações também são basicamente os mesmos do 802.11b e ele é claramente uma tecnologia que, aos poucos, irá substituir as implementações do 802.11b, já que mantém a compatibilidade e oferece maior velocidade. Esta migração já começou e não deve parar tão cedo. Hoje, o custo ainda é mais alto que o do 802.11b, porém esta curva deve se aproximar assim que o mercado começar a usá-lo em aplicações também industriais e robustas.

802.11a

Por causa da grande procura de mais largura de banda, e o número crescente de tecnologias a trabalhar na banda 2,4GHz, foi criado o 802.11a para WLAN a ser utilizado nos Estados Unidos. Este padrão utiliza a freqüência de 5GHz, onde a interferência não é problema. Graças à freqüência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respeitáveis 54 megabits. Note que esta é a velocidade de transmissão nominal que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc. a velocidade real das redes 802.11a é de 24 a 27 megabits por segundo, pouco mais de 4 vezes mais rápido que no 802.11b. Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.
O grande problema é que o padrão também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas. Além disso, por utilizarem uma frequência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.

802.11e

O 802.11e do IEEE fornece melhoramentos ao protocolo 802.11, sendo também compatível com o 802.11b e o 802.11a. Os melhoramentos inclui capacidade multimídia feito possível com a adesão da funcionalidade de qualidade de serviços (QoS – Quality of Service), como também melhoramentos em aspectos de segurança. O que significa isto aos ISP's? Isto significa a habilidade de oferecer vídeo e áudio à ordem (on demand), serviços de acesso de alta velocidade a Internet e Voz sobre IP (VoIP – Voice over Internet Protocol). O que significa isto ao cliente final? Isto permite multimídia de alta-fidelidade na forma de vídeo no formato MPEG2, e som com a qualidade de CD, e a redefinição do tradicional uso do telefone utilizando VoIP. QoS é a chave da funcionalidade do 802.11e. Ele fornece a funcionalidade necessária para acomodar aplicações sensíveis a tempo com vídeo e áudio.

Grupos do IEEE que estão desenvolvendo outros protocolos:

Grupo 802.11d – Está concentrado no desenvolvimento de equipamentos para definir 802.11 WLAN para funcionar em mercados não suportados pelo protocolo corrente (O corrente protocolo 802.11 só define operações WLAN em alguns países).

Grupo 802.11f – Está a desenvolver Inter-Access Point Protocol (Protocolo de acesso entre pontos), por causa da corrente limitação de proibir roaming entre pontos de acesso de diferentes fabricantes. Este protocolo permitiria dispositivos sem fios passar por vários pontos de acesso feitos por diferentes fabricantes.

Grupo 802.11g – Estão a trabalhar em conseguir maiores taxas de transmissão na banda de rádio 2,4GHz.

Grupo 802.11h – Está em desenvolvimento do espectro e gestão de extensões de potência para o 802.11a do IEEE para ser utilizado na Europa.

IEEE 802.11i – trata-se um grupo de trabalho que está ativamente definindo uma nova arquitetura de segurança para WLANs de forma a cobrir as gerações de soluções WLAN, tais como a 802.11a e a 802.11g.

Criptografia e Autenticidade em redes sem fio

Existem duas abordagens recomendadas para autenticação dentro de WLANs. Objetivamente trata-se de realizar a autenticação ou na camada de enlace de dados, ou na camada de rede. A autenticação na camada de enlace é realizada através do uso de WEP. Já a autenticação na camada de rede pode ser realizada através da combinação do uso do protocolo IEEE 802.1x [MA02], que prove a autenticação tanto da estação como da entidade autenticadora.

Formas de autenticação em access points.

Quando se configura um *access point* existem três opções que podem ser usadas para autenticação. São elas:

- Autenticação Aberta (Open Authentication): Onde qualquer estação pode se associar ao access point e obter acesso à rede.
- Autenticação Compartilhada (Shared Authentication): Onde chaves WEP são previamente compartilhadas e estas são usadas para autenticar o cliente junto ao access point. Entretanto, se um dispositivo cliente for furtado, então todas as chaves compartilhadas serão comprometidas e precisarão ser trocadas.
- Rede-EAP (Network-EAP): Existem vários algoritmos EAP (Extensible Authorization Protocol). Estes protocolos dão suporte a autenticação através de servidores Radius.

Beacon Frames

Devidamente especificado no protocolo 802.11. Um *beacon frame* é um frame de sinalização e sincronismo, além de enviar informações importantes a respeito do funcionamento da rede sem fio em questão.

Access points a princípio são configurados de maneira a enviar *beacon frames* no canal em que atuam, bem como no canal subseqüente e antecessor.

A presença destes pacotes pode indicar que *rogue access points* [Air00] estejam ligados à rede. Estes *access points* são instalados sem a autorização e na maioria das vezes representa um grande risco de segurança a rede da instituição.

Ponto de Acesso (Access Point)

Um número limite de estações que podem ser conectadas a cada ponto de acesso depende do equipamento utilizado, mas, assim como nas redes Ethernet, a velocidade da rede cai conforme aumenta o número de estações, já que apenas uma pode transmitir de cada vez. A maior arma do 802.11b contra as redes cabeadas é a versatilidade. O simples fato de poder interligar os PCs sem precisar passar cabos pelas paredes já é o suficiente para convencer algumas pessoas, mas existem mais alguns recursos interessantes que podem ser explorados. Sem dúvidas, a possibilidade mais interessante é a mobilidade para os portáteis. Tanto os notebooks quanto handhelds e as futuras webpads podem ser movidos livremente dentro da área coberta pelos pontos de acesso sem que seja perdido o acesso à rede. Esta possibilidade lhe dará alguma mobilidade dentro de casa para levar o notebook para onde quiser, sem perder o acesso à Web, mas é ainda mais interessante para empresas e escolas. No caso das empresas a rede permitiria que os funcionários pudessem se deslocar pela empresa sem perder a conectividade com a rede e bastaria entrar pela porta para que o notebook automaticamente se conectasse à rede e sincronizasse os dados necessários. No caso das escolas a principal utilidade seria fornecer acesso à Web aos alunos. Esta já é uma realidade em algumas universidades e pode tornar-se algo muito comum dentro dos próximos anos. A velocidade das redes 802.11b é de 11 megabits, comparável à das redes Ethernet de 10 megabits, mas muito atrás da velocidade das redes de 100 megabits. Estes 11 megabits não são adequados para redes com um tráfego muito pesado, mas são mais do que suficientes para compartilhar o acesso à web, trocar pequenos arquivos, jogar games multiplayer, etc. Note que os 11 megabits são a taxa bruta de transmissão de dados, que incluem modulação, códigos de correção de erro, retransmissões de pacotes, etc., como em outras arquiteturas de rede. A velocidade real de conexão fica em torno de 6 megabits, o suficiente para transmitir arquivos a 750 KB/s, uma velocidade real semelhante à das redes Ethernet de 10 megabits.

Mas, existe a possibilidade de combinar o melhor das duas tecnologias, conectando um ponto de acesso 802.11b a uma rede Ethernet já existente. No ponto de acesso da

figura abaixo você pode notar que existem portas RJ-45 da tecnologia Ethernet que trabalham a 100Mbps, veja figura:

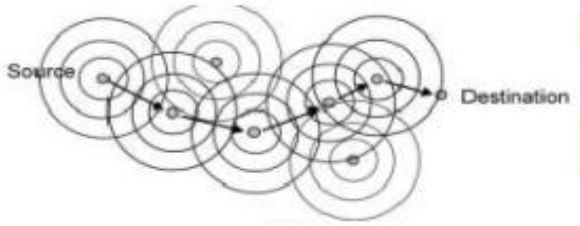
Isto adiciona uma grande versatilidade à rede e permite diminuir os custos. Você pode interligar os PCs através de cabos de par trançado e placas Ethernet que são baratos e usar as placas 802.11b apenas nos notebooks e aparelhos onde for necessário ter mobilidade. Não existe mistério aqui, basta conectar o ponto de acesso ao Hub usando um cabo de par trançado comum para interligar as duas redes. O próprio Hub 802.11b passará a trabalhar como um switch, gerenciando o tráfego entre as duas redes. O alcance do sinal varia entre 15 e 100 metros, dependendo da quantidade de obstáculos entre o ponto de acesso e cada uma das placas. Paredes, portas e até mesmo pessoas atrapalham a propagação do sinal. Numa construção com muitas paredes, ou paredes muito grossas, o alcance pode se aproximar dos 15 metros mínimos, enquanto num ambiente aberto, como o pátio de uma escola o alcance vai se aproximar dos 100 metros máximos.

Redes Ad-Hoc

O termo "ad hoc" é geralmente entendido como algo que é criado ou usado para um problema específico ou imediato. Do Latin, ad hoc, significa literalmente "para isto", um outro significado seria: "apenas para este propósito", e dessa forma, temporário. Contudo, "ad hoc" em termos de "redes ad hoc sem fio" significa mais que isso. Geralmente, numa rede ad hoc não há topologia predeterminada, e nem controle centralizado. Redes ad hoc não requerem uma infra-estrutura tal como backbone, ou pontos de acesso configurados antecipadamente. Os nós ou nodos numa rede ad hoc se comunicam sem conexão física entre eles criando uma rede "on the fly", na qual alguns dos dispositivos da rede fazem parte da rede de fato apenas durante a duração da sessão de comunicação, ou, no caso de dispositivos móveis ou portáteis, por enquanto que estão a uma certa proximidade do restante da rede.

Assim como é possível ligar dois micros diretamente usando duas placas Ethernet e um cabo cross-over, sem usar hub, também é possível criar uma rede Wireless entre dois PCs sem usar um ponto de acesso. Basta configurar ambas as placas para operar em modo Ad-hoc (através do utilitário de configuração). A velocidade de transmissão é a mesma, mas o alcance do sinal é bem menor, já que os transmissores e antenas das interfaces não possuem a mesma potência do ponto de acesso. Este modo pode servir para pequenas redes domésticas, com dois PCs próximos, embora mesmo neste caso seja mais recomendável utilizar um ponto de acesso, interligado ao primeiro PC através de uma placa Ethernet e usar uma placa wireless no segundo PC ou notebook, já que a diferenças entre o custo das placas e pontos de acesso não é muito grande.

Outras características incluem um modo de operação ponto a ponto distribuído, roteamento multi-hop, e mudanças relativamente freqüentes na concentração dos nós da rede. A responsabilidade por organizar e controlar a rede é distribuída entre os próprios terminais. Em redes ad hoc, alguns pares de terminais não são capazes de se comunicar diretamente entre si, então alguma forma de re-transmissão de mensagens é necessária, para que assim estes pacotes sejam entregues ao seu destino. Com base nessas características.



WWAN (Wireless Wide Area Network)

As redes sem fio distribuídas são aquelas usadas pelos sistemas celulares e estão divididas em gerações. A seguir tem-se um estudo das principais redes WWAN.

1G

A primeira geração da telefonia móvel celular usava transmissão de dados analógica. O principal sistema é o AMPS.

2G

A segunda geração de telefonia móvel celular, transmissão de dados passou a ser digital.

2,5G

Nível intermediário entre a 2G e a 3G, permite a conexão de banda larga com celulares e PDAs e oferecem serviços de dados por pacotes e sem necessidade de estabelecimento de uma conexão (conexão permanente) a taxas de até 144 kbps.. Além disso, oferece uma gama de serviços que tornaram esta tecnologia muito mais atraente, como mensagens de texto instantâneas e serviços de localização. Os principais sistemas são o GPRS e extensões do CDMA.

3G

Terceira geração da tecnologia móvel celular. Suas aplicações estão voltadas para o acesso direto à Internet com banda larga, transformando assim o telefone móvel em uma plataforma completa para a obtenção de dados e serviços na internet; além disso, há estudos sobre sua utilização para comércio móvel. Isso significa efetuar compras em máquinas automáticas e lojas utilizando o aparelho celular. Pode operar em freqüências de 1,9 GHz a 2,1 GHz.

Rádio

Sistema utilizado primordialmente em redes públicas, dada a falta de segurança em suas transmissões. É necessário que antenas estejam instaladas dentro do alcance de transmissão, mas nada impede alguém de instalar uma antena para a captação desses dados, que, se não estiverem criptografados adequadamente, poderão ser utilizados para outros fins que não os esperados.
Uma de suas vantagens é que sua operação é feita na freqüência de 2,4 GHz, considerada de uso público, e dessa forma não há a necessidade de autorização de órgãos governamentais para a sua utilização.

GSM

O *Global System for Mobile* é um padrão para telefonia de arquitetura aberta móvel utilizado na Europa e que já esta se espalhando pelo mundo. Ele opera na freqüência de 900 MHz, essa tecnologia esta na sua terceira geração.

QUALIDADE DE SERVIÇOS

Outra forma de ver a camada de transporte é considerar que sua principal função seja melhorar a QoS (Qualidade de Serviço) oferecida pela camada de rede. Se o serviço de rede for perfeito, o trabalho da camada de transporte será fácil. No entanto, se o serviço de rede não for perfeito, a camada de transporte terá que servir de ponte para cobrir a distância entre o que os usuários de transporte desejam e o que a camada de rede oferece.
Ainda que à primeira vista o conceito de qualidade de serviço seja vago (fazer com que todos concordem sobre o que significa um serviço "bom" não é uma tarefa simples), a QoS pode ser definida por um número específico de parâmetros. O serviço de transporte pode permitir ao usuário determinar os valores preferenciais, os valores aceitáveis e os valores mínimos para vários parâmetros de serviço no momento em que uma conexão é estabelecida. Alguns parâmetros também podem ser usados no transporte sem conexão. È tarefa da camada de transporte examinar esses parâmetros e, dependendo do(s) tipo(s) de serviço(s) de rede disponível(eis), determinar se é possível realizar o serviço solicitado. Os parâmetros típicos para a qualidade de serviço da camada de transporte são resumidos em:

- Retardo no estabelecimento da conexão
- Probalidade de falha no estabelecimento da conexão
- Throughput
- Taxa de erros residuais
- Proteção
- Prioridade
- Resiliência

Observe que poucas redes ou protocolos oferecem todos esses parâmetros. Muitas apenas tentam reduzir a taxa de erros da melhor maneira possível. Outras têm arquiteturas de QoS mais elaboradas.
O retardo no estabelecimento da conexão é o tempo transcorrido entre a solicitação de uma conexão de transporte e o recebimento de sua confirmação pelo usuário do serviço de transporte. Nessa característica também está incluído o retardo do processamento na entidade de transporte remota. A exemplo de todos os parâmetros que medem um retardo, quando menor o retardo, melhor o serviço.
A Probabilidade de falha no estabelecimento da conexão é a possibilidade de a conexão não se estabelecer dentro de um período máximo estabelecido devido a, por exemplo, um congestionamento na rede, à falta de espaço de tabela em algum lugar ou a outros problemas internos.
O parâmetro throughput calcula o número de bytes de dados do usuário transmitidos por segundo durante um determinado intervalo de tempo. O throughput é medido separadamente para cada direção.
O retardo de trânsito calcula o tempo transcorrido desde o envio de uma mensagem pelo usuário de transporte da máquina de origem até seu recebimento pelo usuário de transporte da máquina de destino. A exemplo do throughput, cada direção do transporte é analisada separadamente.
A taxa de erros residuais calcula o número de mensagens perdidas ou corrompidas em um porcentagem do total enviado. Na teoria, a taxa de erros residuais deveria ser zero, pois o trabalho da camada de transporte é esconder os erros da camada de rede. Na prática, essa taxa pode apresentar um valor (baixo) finito.
O parâmetro de Proteção oferece uma forma de o usuário de transporte especificar seu interesse no fato de a camada de transporte fornecer proteção contra a leitura, ou a modificação, de dados por parte de terceiros (que se utilizam de "grampos" para violar a comunicação).
O parâmetro de Prioridade oferece ao usuário de transporte um modo de indicar que algumas conexões são mais importantes do que outras e, em caso de congestionamento, garantir que as conexões de maior prioridade sejam atendidas primeiro.
Por fim, o parâmetro de Resiliência oferece à camada de transporte a probabilidade de finalizar uma conexão espontaneamente devido a problemas internos ou a congestionamento.
O parâmetros QoS são especificados pelo usuário de transporte quando uma conexão é solicitada. Os valores mínimo e máximo aceitáveis podem ser fornecidos. Às vezes, ao conhecer os valores de QoS, a camada de transporte percebe imediatamente que alguns deles não podem ser alcançados. Nesse caso, ela informa ao responsável pela chamada que a tentativa de conexão falhou sem sequer tentar contato com o destino. O relatório da falha especifica o que a causou.
Em outros casos, a camada de transporte sabe que não pode alcançar o objetivo desejado (por exemplo, um throughput de 600Mbps), mas pode atingir uma taxa mais baixa, porém aceitável (por exemplo, 150Mbps). Em seguida, a camada de transporte envia a taxa mais baixa e a mínima aceitável para a máquina remota e solicita o estabelecimento de uma conexão. Se a máquina remota não puder administrar o valor sugerido mas conseguir administrar qualquer valor acima do mínimo, a camada de transporte fará uma contraproposta. Se a máquina remota não puder trabalhar com qualquer valor acima do mínimo, ela rejeitará a tentativa de conexão. Por fim, o usuário de transporte da máquina de origem é informado do fato de que a conexão foi estabelecida ou rejeitada. Se a conexão tiver sido estabelecida, o usuário será informado dos valores dos parâmetros acordados.

Esse procedimento é chamado de **negociação de opção** (option negotiation). Uma vez que tenham sido negociadas, as opções serão mantidas durante toda a conexão. Muitas concessionárias de serviços de melhor qualidade para evitar que seus clientes fiquem obcecados por esses detalhes.

QUALIDADE DE SERVIÇOS E DESCRITORES DE TRÁFEGO.

A descrição de QoS é tomada da recomendação E.800, onde define-se a qualidade de serviço como sendo o efeito coletivo provocado pelas características de desempenho de um serviço, determinando o grau de satisfação do usuário. Tal definição engloba, originalmente, vários aspectos de diversas áreas de atuação, incluindo o nível de satisfação do usuário. Na recomendação I.350, o ITU-T achou por bem considerar como parâmetro relevantes para definição da qualidade de serviço na camada ATM, somente aqueles que podem ser diretamente observáveis e mensuráveis no ponto de acesso do serviço dos usuários. Outros tipos de parâmetros não diretamente mensuráveis ou subjetivos em sua natureza não serão tratados como parâmetros para a especificação da QoS. Exemplos de parâmetros utilizados para a definição da QoS na camada ATM são: o retardo, a sensibilidade à variação estatística do retardo, a taxa de perda de células etc. A tradução da QoS específica da aplicação para a QoS adequada da camada ATM é papel das camadas superiores de protocolo, incluindo a AAL.

O desempenho da rede (NP) é medido em termos de parâmetros utilizáveis pelo provedor dos serviços de comunicação com o propósito de projeto, configuração, operação e manutenção do sistema. Os objetivos do desempenho de rede em um SAP ATM são definidos para capturar a capacidade da rede em atender a qualidade de serviço requerido da camada ATM. As noções de QoS e NP diferem quanto ao propósito e enfoque dos parâmetros que as caracterizam. Os parâmetros de QoS são definidos sob o ponto de vista do usuário de um determinado serviço, enquanto que os parâmetros de NP são definidos sob o ponto de vista da infra estrutura de comunicação que fornece suporte ou implementa esse serviço. Ambos os parâmetros são necessários, e os seus valores devem estar quantitativamente relacionados para que a rede possa servir efetivamente aos seus usuários.

A definição dos parâmetros de QoS e NP deve tornar claro o mapeamento entre os seus valores em todos os casos onde esse mapeamento não for um para um.

Tais mecanismos têm como principal objetivo garantir a manutenção da qualidade de serviço especificada e desejada pelos usuários no momento em que uma conexão ATM é estabelecida. Uma RDSI-FL deverá fornecer um determinado número de classes de serviço, cada uma associada a uma qualidade de serviço e seus parâmetros – cada conjunto de parâmetros e seus valores determina uma QoS. Adicionalmente, dentro de cada classe, característica particulares de capacidade podem ser especificadas.

Um usuário requisita uma QoS específica da camada ATM através das classes QoS que a rede fornece. Isso deve fazer parte do contrato de tráfego definido no estabelecimento da conexão. È responsabilidade da rede garantir a qualidade de serviço negociada, desde que o usuário cumpra a sua parte no contrato de tráfego. Se o usuário violar o contrato , a rede pode não respeitar a QoS acordada.

Um usuário pode requisitar até duas classes diferentes de QoS para uma conexão ATM cada uma associada à uma taxa de perda das células (cell loss ratio – CLR). O bit de prioridade de perda de célula, por nós visto quando estudamos o cabeçalho de uma célula ATM, definirá os parâmetros QoS que deverão ser atendidos para a célula em questão.

Parâmetros de tráfego – descrevem as características de tráfego de uma conexão ATM.

Parâmetros de tráfego são agrupados em descritores de tráfego da fonte para a troca de informação entre o usuário e a rede. Podemos, assim, definir mais precisamente os descritos de tráfego como uma lista genérica de parâmetros de tráfego que podem ser utilizados para capturar as características de uma conexão ATM. Exemplos de parâmetros de tráfego são: taxa de pico de geração de células (cell peak rate), taxa média de transferência de células (avarage cell rate),duração de um pico (peak duration),explosividade (burstiness) e tipo de fonte (telefone, videofone etc.).

Se o usuário requerer dois níveis de prioridade para a conexão ATM, conforme indicado pelo bit CLP do cabeçalho de uma célula, as características intrínsecas de tráfego do fluxo de ambos os tipos de células devem ser especificados no descritor de tráfego da fonte. Isto é feito por meio de um conjunto de parâmetros de tráfego associado com as células CLP=0, e um conjunto de parâmetros de tráfego associado com todas as células (isto é CLP=0+1).

Os procedimentos de controle de admissão fazem uso dos descritos de tráfego da fonte para a alocação de recursos e para derivar parâmetros para a operação dos mecanismos de policiamentos da fonte. Todo parâmetro de tráfego de um descritor de tráfego da fonte deve ser enquadrado pelos mecanismos de policiamento.

Os algoritmos de controle de tráfego e congestionamento requerem o conhecimento de certos parâmetros para atuarem eficientemente. Eles devem levar em consideração o descritor de tráfego da fonte, a QoS requerida e a tolerância máxima à variação de retardo da célula – tolerância máxima CDV (cell delay variation) – para decidir se uma conexão requerida pode ser aceita(isto é, se uma determinada QoS pode ser atendida.)

As funções de uma camada ATM (por exemplo, a multiplexação de células) pode alterar as características de tráfego de uma conexão ATM pela introdução de uma variação do retardo. Quando células de duas ou mais conexões ATM são multiplexadas, as células de uma dada conexão podem ser retardadas enquanto células de outra conexão estão sendo inseridas na saída do multiplexador. Células também podem sofrer retardos devido ao overhead do nível físico ou a introdução de células OAM no fluxo de saída do multiplexador.

Assim, alguma aleatoriedade pode ser introduzida no intervalo de tempo entre células no ponto final de uma conexão ATM. Além disso, a multiplexação AAL pode também originar a variação de retardo de células (CDV). Ora, os mecanismos de policiamento não devem descartar, ou marcar para descartar, células geradas pela fonte em acordo com o descritor de tráfego negociado. Contudo, se a CDV não for limitada no ponto onde o mecanismo de

controle de policiamento é executado, não é possível projetar um mecanismo adequado (taxas de células são aumentadas e diminuídas não pela fonte, mas pela CDV, o que pode causar a ilusão de que a taxa de pico de uma fonte de tráfego está sendo violada), nem fazer o uso de uma alocação de recursos apropriada. Assim, é importante que um valor máximo para a CDV seja estabelecido ente o SAP da conexão ATM e a interface TB, entre a interface TB e a interface NNI, e entre interfaces NNI. Esses valores devem ser levados em conta nos mecanismos de controle de tráfego e congestionamento. O descritor de tráfego da fonte, a QoS requerida e a tolerância máxima CDV alocada a um equipamento do usuário definem o contrato e tráfego em um ponto de referência TB. O descritor de tráfego da fonte e a QoS requerida são declaradas pelo usuário no estabelecimento da conexão, por meio de sinalização ou subscrição. Se a tolerância máxima CDV é também negociada na subscrição ou por conexão é assunto ainda em estudo.
A taxa de pico de geração de células e a tolerância máxima CDV são parâmetros obrigatórios em um contrato de tráfego. Parâmetros adicionais podem prover uma melhora significativa da utilização da rede.

POR QUE QoS?
Na internet e nas intranets atuais, a largura de banda é um assunto importante. Mais e mais pessoas estão usando a Internet por motivos comerciais e particulares. O montante de dados que precisa ser transmitido através da internet vem crescendo exponencialmente. Novos aplicativos, como RealAudio, RealVideo, Internet Phone e sistemas de videoconferência precisam cada vez de mais largura de banda que os aplicativos usados nos primeiros anos da Internet. Enquanto que aplicativos Internet tradicionais, como WWW, FTP ou Telnet, não toleram perda de pacotes, mas são menos sensíveis aos retardos variáveis, a maioria dos aplicativos em tempo real apresenta exatamente o comportamento oposto, pois podem compensar uma quantidade razoável de perda de pacotes mas são, normalmente, muito críticos com relação aos retardos variáveis.
Isso significa que sem algum tipo de controle de largura de banda, a qualidade desses fluxos de dados em tempo real dependem da largura de banda disponível no momento.
Larguras de banda baixas, ou mesmo larguras de banda melhores mas instáveis, causam má qualidade em transmissões de tempo real, com eventuais interrupções ou paradas definitivas da transmissão. Mesmo a qualidade de uma transmissão usando o protocolo de tempo real RTP depende da utilização do serviço de entrega IP subjacente.
Por isso, são necessários conceitos novos para garantir uma QoS específica para aplicativos em tempo real na Internet. Uma QoS pode ser descrita como um conjunto de parâmetros que descrevem a qualidade (por exemplo, largura de banda, utilização de buffers, prioridades, utilização da CPU etc.) de um fluxo de dados específico. A pilha do protocolo IP básica propicia somente uma QoS que é chamada de melhor tentativa. Os pacotes são transmitidos de um ponto a outro sem qualquer garantia de uma largura de banda especial ou retardo mínimo. No modelo de tráfego de melhor tentativa, as requisições na Internet são processadas conforme a estratégia do primeiro a chegar, primeiro a ser atendido. Isso significa que todas as requisições têm a mesma prioridade e são processadas uma após da outra. Não há possibilidade de fazer reserva de largura de banda para conexões específicas ou aumentar a prioridade de uma requisição especial. Assim, foram desenvolvidas novas estratégias para oferecer serviços previsíveis na Internet.

Hoje em dia, há dois princípios básicos para conseguir QoS na Internet:

- **Serviços integrados**
- **Serviços diferenciados**

Os serviços integrados trazem melhoramentos ao modelo de rede IP para suportar transmissões em tempo real e garantir largura de banda para seqüências de dados específicas. Neste caso, definimos um fluxo de dados (stream) como uma seqüência distinguível de datagramas relacionados transmitidos de um único emissor para um único receptor que resulta de uma única atividade de usuário e requer a mesma QoS.
Por exemplo, um fluxo de dados poderia consistir de um stream de vídeo entre um par de host determinado. Para estabelecer a conexão de vídeo nas duas direções, são necessários dois fluxos de dados.
Cada aplicativo que inicia um fluxo de dados pode especificar a QoS exigida para esse fluxo. Se a ferramenta de videoconferência precisar de uma largura de banda mínima de 128 Kbps e um retardo de pacote mínimo de 100 ms para garantir exibição de vídeo contínua, essa QoS pode ser reservada para essa conexão.
O mecanismo de Serviços Diferenciados não usa sinalização por fluxo. Níveis diferentes de serviços podem ser reservados para grupos diferentes de usuários da Internet, o que significa que o tráfego todo será dividido em grupos com parâmetros de QoS´s diferentes.
Isso reduz a carga extra de manutenção em comparação com os Serviços Integrados.

TRANSMISSÃO MULTIMÍDIA EM REDES
Pode-se dividir a parte de transmissão multimídia em redes de computadores como mostra a figura abaixo, ou seja, a parte de conferência (que requer interatividade) e a parte de transmissão de vídeo (que envolve apenas um lado transmitindo e vários clientes recebendo). Ambas possuem necessidades diferentes para funcionarem a contento, por exemplo, as aplicações de conferência normalmente possuem necessidades mais rígidas em relação ao atraso da rede, enquanto que a transmissão unidirecional pode trabalhar com um atraso maior.

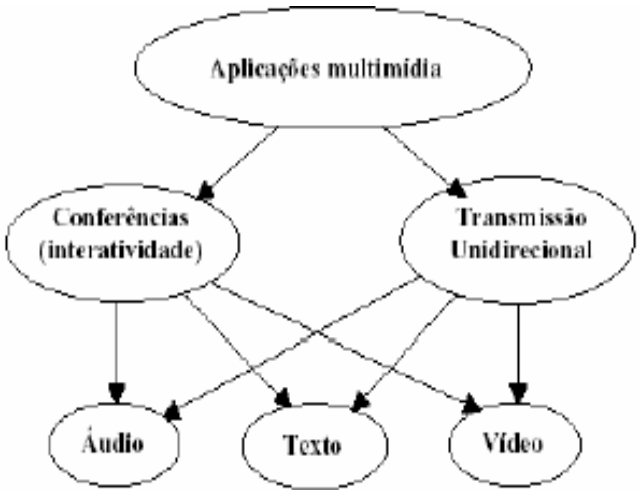


Figura – Transmissão multimídia em rede

Necessidades das aplicações (latência, jitter, skew, tabela Comparativa)

Atualmente existe uma tendência de convergência de aplicações em um único meio físico, ou seja, voz, vídeo, dados, imagens, músicas, e tudo que possa ser transformado em bits utilizando o mesmo meio físico. Entretanto, as aplicações tem características e necessidades bem diferentes umas das outras, como por exemplo voz, que exige latência e *jitter* baixos, dados, que não tem tanta preocupação com latência e *jitter*, e videoconferência, que além de exigir latência e *jitter* baixos, ainda necessita de *skew* baixo, a fim de manter sincronizados voz e vídeo. A seguir será feita a definição desses termos, e depois será mostrada uma tabela comparativa das necessidades das aplicações.

Latência

Em redes de computadores, latência é o tempo que um pacote leva da origem ao destino.

Caso esse atraso seja muito grande, prejudica uma conversação através da rede, tornando difícil o diálogo e a interatividade necessária para certas aplicações. Segundo alguns estudos, um atraso confortável para o ser humano fica na ordem de 100ms. Suponha duas pessoas conversando através da Internet. À medida que o atraso aumenta, as conversas tendem a se entrelaçar, ou seja, uma pessoa não sabe se o outro a ouviu e continua falando. Após alguns milisegundos vem a resposta do interlocutor sobre a primeira pergunta efetuada, misturando as vozes. Num atraso muito grande, as pessoas devem começar a conversar utilizando códigos, tipo "câmbio", quando terminam de falar e passam a palavra ao outro. Os principais responsáveis pela latência são o atraso de transmissão, de codificação e de empacotamento, que podem ser definidos da seguinte forma:

Atraso de transmissão: tempo após a placa de rede ter transmitido o pacote até ele chegar na placa de rede do computador destino. Esse tempo envolve uma série de fatores, como o atraso no meio físico (por exemplo fibra ótica, UTP, *wireless*), processamento em cada roteador ou switch intermediário (por exemplo, para trocar o TTL do pacote e decidir sua rota), fila de espera em cada roteador e switch intermediário, e assim por diante;

Atraso de codificação e decodificação: sinais como voz e vídeo normalmente são codificados em um padrão, tipo PCM (G.711 a 64Kbps) para voz, ou H.261 para vídeo.
Essa codificação gasta um tempo de processamento na máquina. Alguns protocolos gastam menos, como o G.711, que ocupa menos de 1ms de codificação /PAS 97a/, porém, requer 64Kbps de banda. Alguns protocolos de voz, como o G.729, requerem 25ms de codificação, mas ocupam apenas 8Kbps de banda;

Atraso de empacotamento e desempacotamento: após codificado, o dado deve ser empacotado na pilha OSI a fim de ser transmitido na rede, e isso gera um atraso. Por exemplo, numa transmissão de voz a 64Kbps, ou 8000 bytes por segundo, tem-se que, para preencher um pacote de dados contendo apenas 100 bytes, vai levar 12,5ms. Mais 12,5ms serão necessários no destino a fim de desempacotar os dados. Além da latência, a existência do *jitter* é outro fator de atraso na comunicação entre duas pessoas.

JITTER

Utilizar somente a latência não é suficiente para definir a qualidade de transmissão, pois as redes não conseguem garantir uma entrega constante de pacotes ao destino. Assim, os pacotes chegam de forma variável, como mostra a figura 2.2, ocasionando o *jitter*, que nada mais é do uma flutuação na latência, ou variação estatística do retardo.

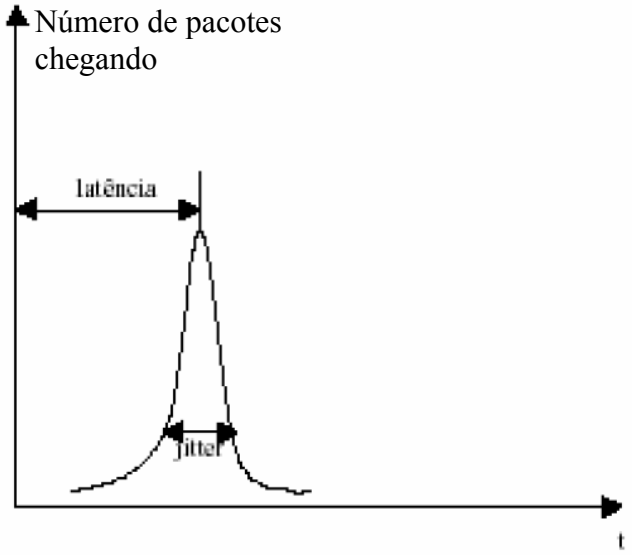


Figura – Comparação entre latência e jitter

A conseqüência do *jitter* é que a aplicação no destino deve criar um *buffer* cujo tamanho vai depender do *jitter*, gerando mais atraso na conversação. Esse buffer vai servir como uma reserva para manter a taxa de entrega constante no interlocutor. Daí a importância de latência e *jitter* baixos em determinadas aplicações sensíveis a esses fatores, como videoconferência.

"Skew"

O *skew* é um parâmetro utilizado para medir a diferença entre os tempos de chegada de diferentes mídias que deveriam estar sincronizadas, como mostra a figura 2.3. Em muitas aplicações existe uma dependência entre duas mídias, como áudio e vídeo, ou vídeo e dados. Assim,

numa transmissão de vídeo, o áudio deve estar sincronizado com o movimento dos lábios (ou levemente atrasado, visto que a luz viaja mais rápido que o som, e o ser humano percebe o som levemente atrasado em relação à visão).

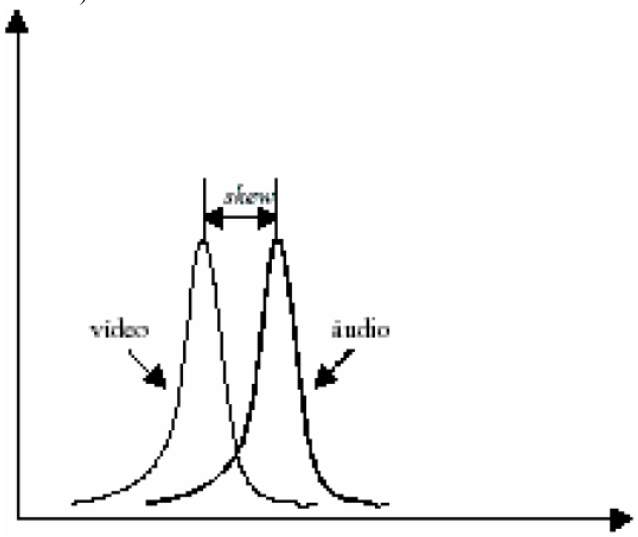


Tabela comparativa

A tabela a seguir mostra algumas aplicações típicas em rede, bem como seus fatores críticos, em aplicações numa tendência de convergência nas redes.

	Telefone	**Download**	**TV**	**Vídeo conferencia**
Latência	Sensível	Insensível	Insensível	Sensível
Jitter	Sensível	Insensível	Sensível	Sensível
Skew	-	Insensível	Sensível	Sensível
Velocidade (largura de banda)	Baixa	Depende	Alta	Alta

Aplicações de telefonia são sensíveis a latência e *jitter*. Caso estiverem associadas a sincronismo em alguma figura, como por exemplo um áudio explicativo associado a uma seta se movendo numa figura, o áudio também é sensível a *skew*. Possuem velocidade baixa, de 64Kbps no padrão G.711, o mais comum em telefonia atualmente, mas pode-se chegar a apenas 8Kbps, usando a compressão no padrão G.729.

Aplicações de *download* de dados são insensíveis a latência, *jitter* e *skew*, podem variar em necessidades de velocidade, e possuem taxa variável. Entretanto, na maior parte das vezes esse tipo de mídia não pode sofrer perdas. Pode-se imaginar o problema que pode acontecer de perdas de pacotes numa transação bancária. Já em transmissões unilaterais de áudio e vídeo, como por exemplo TV, a latência não é tão importante, visto que não vai fazer muita diferença se a transmissão demorar 5 segundos para começar a passar. Entretanto, uma vez que começou, deve se manter até o final e com sincronismo entre áudio e vídeo, daí a necessidade de *jitter* e *skew* baixos. Aplicações de videoconferência são muito parecidas com aplicações de voz em termos de latência e *jitter*, entretanto, possuem alta largura de banda e devem manter um baixo *skew*, pois necessitam sincronização entre áudio e vídeo.

QUALIDADE DE SERVIÇO (REQUISITOS GERAIS PARA SUPORTE A SERVIÇO BANDA LARGA)

A camada de transporte tem como uma das principais funções a ampliação da qualidade de serviço (Quality of Service – QoS) fornecida pela camada de rede. A qualidade de serviço pode ser caracterizada por uma série de parâmetros específicos (parâmetros QoS). Entre estes podemos citar:

- O retardo no estabelecimento da conexão.
- O retardo no encerramento da conexão.
- A probabilidade de falha no estabelecimento da conexão. Isto é, a probabilidade que uma conexão não seja estabelecida dentro do retardo máximo de estabelecimento.
- A probalidade de falha na liberação da conexão. Isto é, a fração das tentativas de liberação de conexões que não se completaram dentro do retardo máximo de encerramento.
- A vazão em cada sentido da conexão, isto é, a taxa de bits transferidos por segundo.
- O retardo de transferência médio, também em cada sentido.
- A variação estatística do retardo, expressa, por exemplo, em termos da variância do retardo de transferência.
- A taxa de erro, expressa em porcentagem dos bits transmitidos.
- A prioridade de queda de uma conexão, isto é, a probabilidade de que a camada de transporte. O serviço de transporte permite ao usuário especificar valores preferencias, valores aceitáveis e inaceitáveis, quando do estabelecimento de uma conexão. Alguns dos parâmetros se aplicam tanto ao serviço com conexão quanto ao serviço sem conexão. É função da camada de transporte examinar os parâmetros requeridos e determinar se pode ou não fornecer o serviço.
- A definição da camada de transporte RM-OSI não determina a codificação ou os valores permitidos para os parâmetros QoS.

ANÁLISE DE SERVIÇOS QoS

GARANTIA DE QoS

Somente o aumento na largura de banda não é suficiente para garantir a qualidade do serviço à aplicação, pois em se tratando de redes compartilhadas por múltiplos usuários e muitas vezes a longas distâncias, podem haver congestionamentos, provocando atrasos inadmissíveis em certas aplicações sensíveis, como por exemplo voz e videoconferência.

Existem algumas formas de prover qualidade de serviço às aplicações críticas: serviços integrados, serviços diferenciados, prioridade relativa e *label switching*.

Serviços Diferenciados

Ao contrário dos serviços integrados, descrito mais adiante, os padrões que utilizam serviços diferenciados preenchem um campo específico no pacote para dizer a prioridade que a aplicação tem. Assim, cada nó da rede pode priorizar ou não o encaminhamento do pacote. O diffserv, visto a seguir, é um exemplo dessa arquitetura.

Differentiated Services (diffserv)

O objetivo da arquitetura diffserv é melhorar o protocolo IP a fim de obter qualidade de serviço de uma forma escalável, ou seja, sem depender de protocolos de sinalização em cada nó ou reserva de recursos baseada em fluxo. Para isso, é utilizado o campo DS (*Differentiated Services*) do cabeçalho IP, que nada mais é do que o campo TOS (*Type Of Service*) do cabeçalho IPv4 (RFC 791) ou o campo "classe de tráfego" do IPv6 (RFC 2460). A configuração do campo DS pela aplicação vai determinar o comportamento do pacote na rede e seu tipo de serviço, ou seja, se ele vai ser mais ou menos prioritário.

Serviços são definidos como necessidades dos usuários, tanto fim a fim como dentro de um mesmo domínio. Tais necessidades podem ser de largura de banda ou baseadas em desempenho relativo (uso de classes). O contrato de serviço entre o cliente e o provedor de serviços é conhecido como *Service Level Agreement* (SLA). Os serviços podem ser implementados de acordo com as seguintes diretivas:

- Marcar o campo DS do cabeçalho IP de acordo com o tipo de serviço. Usado nos limites da rede (limites de sistemas autônomos, limites administrativos internos ou *hosts*);
- Usar o campo DS para determinar a prioridade com que os pacotes serão encaminhados através dos nós da rede;
- Condicionar os pacotes nos limites da rede de acordo com os requerimentos de cada serviço, como por exemplo monitoramento, política e conformação de tráfego. Dessa forma, cada pacote vai ter um comportamento num determinado nó, e isso é conhecido como "*per-hop behaviors*", ou PHB. Muitos padrões de PHB estão em desenvolvimento no IETF, como por exemplo o *Expedited Forwarding* (EF), ou "encaminhamento agilizado", e *Assured Forwarding* (AF), ou "encaminhamento garantido" . O campo DS é mostrado na figura abaixo Como pode ser visto, seis bits são usados como código para determinar o PHB que determinado pacote vai ter em cada nó da rede. Dois bits não são usados ainda.

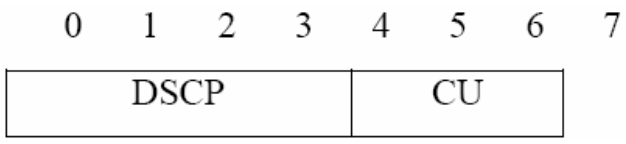


Figura – Estrutura do campo DS

DSCP: differentiated services codepoint
CU: Currently Unused

O campo DS visto acima é incompatível com a estrutura definida no campo TOS do IPv4, podendo provocar comportamentos de encaminhamento de pacotes indesejáveis caso o pacote seja IPv4 original. Para eliminar esse problema, está definido um método de utilização do DS onde existe uma compatibilização ao campo TOS.

Serviços Integrados

O grupo de trabalho de serviços integrados do IETF desenvolveu um modelo que inclui serviços de **melhor esforço** e de **tempo real**, descrito na RFC 1633. O serviço de tempo real é utilizado para prover qualidade de serviço em aplicações multimídia sobre redes IP.

O protocolo RSVP (*Resource Reservation Protocol*) permite uma reserva de recursos ao longo do caminho entre origem e destino, e será analisado a seguir.

Resource Reservation Protocol

RSVP é um protocolo de controle que roda sobre IP, ocupando o lugar do protocolo de transporte, da mesma forma que o ICMP, IGMP ou protocolos de roteamento. As aplicações utilizam RSVP para reservar e manter durante a conexão uma determinada qualidade de serviço até a aplicação destino, e o RSVP faz isso criando um caminho entre origem e destino, perguntando a todos os nós intermediários se eles suportam a qualidade desejada, e reservando as necessidades daquela aplicação. Para tanto, todos os nós no meio do caminho devem suportar esse protocolo. O protocolo RSVP utiliza outros protocolos para efetuar roteamento e transmissão. Seu objetivo único é a reserva, manutenção e liberação de recursos quando solicitado. Assim, pode operar em unicast, multicast, Ipv4, Ipv6, e outros. A figura abaixo mostra os módulos necessários em uma implementação RSVP, e em seguida se tem um resumo deles.

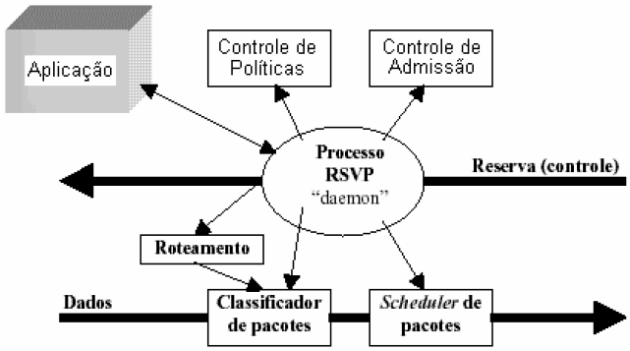


Figura – Módulos necessários em uma implantação RSVP.

- **Controle de admissão**: utilizado no início da chamada para verificar se o nó tem recursos suficientes para atender a qualidade de serviço solicitada;
- **Controle de políticas**: determina se o usuário tem permissão administrativa para fazer a reserva;
- **Classificador e *scheduler* de pacotes**: o classificador de pacotes determina a classe de QoS. Quando a solicitação passa pelo controle de admissão e políticas, são configurados alguns parâmetros nesses módulos, a fim deles reconhecerem os pacotes para ordenar corretamente na saída, dando a necessária qualidade de serviço para cada fluxo;

- **Fluxo de dados**: RSVP é simplex, ou seja, faz reservas para fluxos unidirecionais.

O processo do RSVP também se comunica com as rotinas de roteamento para determinar o caminho das solicitações de reserva. Isso causa um problema no caso de mudança de uma rota na tabela de roteamento (que é dinâmica), gerando uma necessidade de reserva (feita automaticamente) através do novo caminho. Para conseguir isso, o caminho estabelecido é do tipo "*soft state*", necessitando mensagens periódicas para se manter. Na ausência de tais mensagens (por uma mudança de rota ou saída de cliente), a interface dá *time-out* e a reserva é liberada. A reserva de QoS é feita na ordem reversa, ou seja, do receptor ao transmissor. Essa solicitação de reserva se repete até que chegue no transmissor ou encontre um nó com as mesmas necessidades. Tais reservas são implementadas através de dois tipos de mensagens: PATH e RESV.

- **PATH**: mensagens enviadas periodicamente pelo transmissor ao endereço multicast. Contém a especificação de fluxo (formato de dados, endereço fonte, porta fonte) e características de tráfego. Essa informação é utilizada pelos receptores para achar o caminho reverso ao transmissor e determinar quais recursos devem ser reservados. Os receptores devem se cadastrar no grupo multicast a fim de receber mensagens PATH;
- **RESV**: mensagens geradas pelos receptores contendo parâmetros de reserva, como especificação de fluxo e de filtro. O filtro determina quais pacotes no fluxo de dados devem ser usados no classificador de pacotes. A especificação de fluxo é usada no *scheduler*, que procura manter a necessidade do receptor.

Prioridade Relativa

No modelo de prioridade relativa, a aplicação configura uma determinada prioridade (ou precedência) para o pacote, e os nós ao longo do caminho aplicam essa regra na hora de encaminhar o quadro. O comportamento que pode ser configurado é de atraso relativo ou prioridade de descarte. A arquitetura Diffserv pode ser considerada um refinamento desse modelo, pois especifica com maiores detalhes a importância dos domínios de tráfego, bem como os condicionadores de tráfego. Alguns exemplos desse tipo de QoS são o modelo de precedência do IPv4 definido na RFC 791, a prioridade das redes Token Ring (IEEE 802.5) e a interpretação das classes de tráfego dada no protocolo IEEE 802.1p, que será analisado a seguir.

Protocolo IEEE 802.1p/Q

O protocolo IEEE 802.1p é uma técnica para priorização de tráfego em redes locais, sendo especificado na norma IEEE 802.1D – LAN Bridges /CON 99/. Através dessa técnica, é possível utilizar aplicações sensíveis a tempo em ambientes LAN. No IEEE 802.1p, estão definidas 8 classes de tráfego. Como os pacotes Ethernet não possuem campos para priorização de tráfego, a norma 802.1p recomenda a utilização da extensão Ethernet para reconhecimento de VLANs, definida na norma 802.1Q. Essa norma adiciona 4 bytes ao pacote Ethernet a fim de reconhecimento de VLANs, e desses 4 bytes, 3 bits são reservados para priorização de tráfego.

Classes de serviço no ATM

No ATM, a qualidade de serviço está especificada na camada AAL (ATM Adaptation Layer). Como as aplicações possuem necessidades diferentes, o ITU definiu grupos de aplicações com requisitos semelhantes, baseado em três critérios:

- **Temporização entre origem e destino**: necessária ou não necessária;
- **Taxa de bit**: constante ou variável;
- **Modo de conexão**: orientado à conexão ou não.

SERVIÇOS INTEGRADOS

O modelo de serviços integrados (IS, Integrated Services) foi definido por um grupo de trabalho da IETF a fim de ser a pedra angular da Internet IS planejada. Esse modelo de arquitetura Internet inclui o serviço de melhor tentativa usado atualmente e um novo serviço em tempo real que disponibiliza funções para reservar larguras da banda na Internet.

O IS foi desenvolvido para otimizar a utilização de redes e recursos para novos aplicativos, como multimídia em tempo real, que requer garantias de QoS. Devido aos retardos de roteamento e perdas devido ao congestionamento, os aplicativos em tempo real não funcionam muito bem na Internet atual que usa o método da melhor tentativa. Os programas de videoconferência, transmissão de vídeo e conferências usando áudio precisam de larguras de banda garantidas a fim de obter qualidade aceitável de vídeo e de áudio. Os serviços integrados tornam isso possível dividindo o tráfego da Internet no tráfego da melhor tentativa padrão para uso tradicional e no tráfego de fluxos de dados de aplicativos como QoS garantida.

Para suportar o modelo de serviços integrados, um roteador da Internet precisa ser capaz de propiciar uma QoS apropriada para cada fluxo de dados, de acordo com o modelo do serviço. A função do roteador que propicia qualidades diferentes de serviços é chamada de controle de tráfego. Ela consiste dos seguintes componentes:

Programador de Pacotes

O programador de pacotes controla o direcionamento de fluxos de pacotes deferentes em hosts e roteadores com base em suas classes de serviço, usando gerenciamento de filas e vários algoritmos de programação. Ele precisa garantir que a entrega do pacote corresponda ao parâmetro de QoS de cada fluxo. Um programador de pacotes também pode policiar ou moldar o tráfego de acordo com o nível de serviços. Ele precisa ser implementado no ponto onde os pacotes são enfileirados. Esse é normalmente o nível do driver de saída em um sistema operacional e corresponde ao protocolo de camada de enlace.

Classificador de Pacotes

O classificador de pacotes identifica os pacotes de um fluxo IP em hosts e roteadores que irão receber um certo nível de serviço. Para realizar um controle efetivo de tráfego, cada pacote de entrada é mapeado pelo classificador em uma classe específica. Todos os pacotes que são classificados na mesma classe obtêm o mesmo tratamento por parte do programador de pacotes. A escolha de uma classe se baseia nos endereços de origem e de destino e no número da porta no cabeçalho do pacote existente ou em um número de classificação adicional que precisa ser adicionado a cada pacote. Uma classe pode corresponder a uma ampla categoria de fluxos de dados. Por exemplo, todos os fluxos de vídeo de uma videoconferência com vários participantes podem pertencer a uma classe de serviço. Mas também é possível que apenas um fluxo pertença a uma classe específica de serviço.

Controle de Admissão

O controle de admissão contém o algoritmo de decisão que um roteador usa para determinar se há recursos de roteamento suficientes a fim de aceitar a QoS solicitada para um novo fluxo de dados. Se não houver recursos de roteamento livres suficientes, a aceitação de um fluxo novo de dados iria prejudicar garantias anteriores e o novo fluxo precisa ser rejeitado. Se o novo fluxo for aceito, a solicitação de reserva no roteador designa o classificador de pacotes e o programador de pacotes para reservarem a QoS reservada para esse fluxo. O controle de admissão é chamado em cada roteador ao longo do caminho de reserva, para tomar uma decisão de aceitação/rejeição na hora que um host requisitar um serviço de tempo real. O algoritmo de controle de admissão precisa serconsistente com o modelo do serviço.

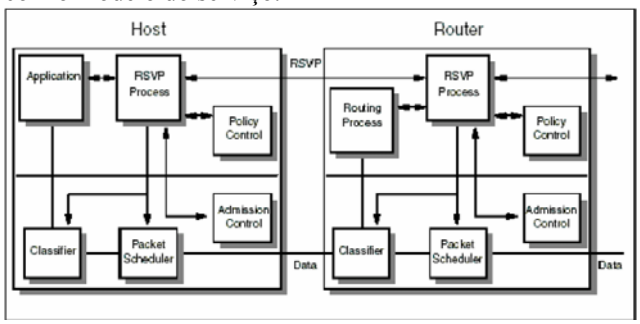


Figura – Modelo de Serviços Integrados.

Note que o controle de admissão algumas vezes torna-se confuso com a fiscalização, que é uma função pacote a pacote processada pelo programador de pacotes. Ela garante que um host não viole suas características de tráfego definidas. Apesar disso, para garantir que as garantias de QoS sejam honradas, o controle de admissão estará preocupado com o esforço das políticas administrativas sobre as reservas de recursos. Algumas políticas serão usadas para verificar a autenticação dos usuários para uma reserva requisitada. Requisições de reservas não autorizadas podem ser rejeitadas. O controle de admissão terá um papel importante nos custos dos recursos da Internet no futuro. A figura 3.3 mostra a operação do modelo de serviços integrados em um host e em um roteador.

Os serviços integrados usam o RSVP (Reservation Protocol – protocolo de reserva) para a sinalização das mensagens de requisição de reservas. As instâncias IS se comunicam via RSVP para criar e manter estados de fluxos específicos nos hosts dos pontos terminais e nos roteadores ao longo do caminho de um fluxo de dados.

O aplicativo que quiser enviar pacotes de dados em um fluxo reservado, se comunica com a instância de fazer reservas RSVP. O protocolo RSVP tenta fazer uma reserva de fluxo com a QoS solicitada, a qual será aceita se o aplicativo atender às restrições do plano de ação e os roteadores puderem lidar com a QoS requisitada. O RSVP informa ao classificador de pacotes e ao programador de pacotes em cada nó para processar os pacotes desse fluxo adequadamente. Se o aplicativo enviar agora os pacotes de dados para o classificador no primeiro nó, o qual classificou esse fluxo em uma classe de serviço específica de acordo com a QoS solicitada, o fluxo será reconhecido como o endereço IP do emissor e será transmitido para o programador de pacotes. Este encaminha os pacotes, dependendo de suas classes de serviço, para o roteador seguinte ou, finalmente, para o host de recepção.

Como o RSVP é um protocolo simplex, as reservas de QoS são feitas somente em uma direção, do nó emissor para o nó receptor. Se o aplicativo de nosso exemplo quiser cancelar a reserva do fluxo de dados, ele envia uma mensagem para a instância de reserva que libera os recursos da QoS reservados em todos os roteadores ao longo do caminho, podendo então esses recursos serem usados para outros fluxos de dados. As especificações IS estão definidas na RFC 1633.

Classes de serviços

O modelo de serviços integrados usa classes diferentes de serviços que são definidas pelo grupo de trabalho IETF de serviços integrados. Dependendo do aplicativo, essas classes de serviços propiciam limites mais estreitos ou tolerantes nos controles de QoS. O modelo IS atual inclui o Guaranteed Service (serviço garantido) definido na RFC 2212 e o Controlled Load Service (serviço de carga controlada) definido na RFC 2211. Para entender essas classes de serviços, alguns termos precisam ser aplicados.

Como o modelo IS fornece reservas por fluxo, a cada fluxo é atribuído um descritor de fluxo. Este define as características de tráfego e QoS para um fluxo específico de pacotes de dados. Nas especificações IS, o descritor de fluxo consiste de uma especificação de filtro e uma especificação de fluxo.

A especificação de filtro é usada para identificar os pacotes que pertencem a um fluxo específico com o endereço IP do emissor e a porta de origem. A informação da especificação de filtro é usada no classificador de pacotes. A especificação de fluxo contém um conjunto de parâmetros que são chamados de informação de chamada. È possível ordenar a informação de chamada em dois grupos:

- Especificação de Tráfego (Tspec)
- Especificação de Requisição (Rspec)

A especificação de tráfego descreve as características de tráfego requisitado. No modelo IS essa especificação é

representada por um filtro chamado de token bucket (balde de fichas).
Esse princípio define um mecanismo de controle de fluxo de dados que adiciona fichas (tokens) em intervalos de tempo periódicos em um buffer (o balde – bucket) e permite que um pacote de dados deixe o emissor somente se houver pelo menos tantas fichas no balde quanto o comprimento do pacote de dados. Essa estratégia permite um controle preciso do intervalo entre dois pacotes de dados na rede. Esse sistema é especificado por dois parâmetros : a taxa de fichas ® que representa a taxa na qual as fichas são colocadas no balde e a capacidade do balde(b). Ambos, r e b têm que ser valores positivos.
O parâmetro r especifica a taxa de dados a longo prazo e é medida em bytes de datagramas IP por segundo. O valor desse parâmetro pode variar de 1 byte por segundo a até 40 terabytes por segundo. O parâmetro b especifica o montante de dados momentâneo permitido pelo sistema e é medido em bytes. O valor desse parâmetro pode variar de 1 bytes a 250 gigabytes. As faixas de valores permitidas para esses parâmetros são propositadamente grandes para que o sistema esteja preparado para as tecnologias de rede do futuro. Não se espera que os elementos de rede suportem essa faixa tão ampla de valores. O tráfego que passa pelo filtro do balde de fichas tem que obedecer à regra de que, durante todos os períodos T de tempo, o montante de dados enviados não deve exceder rT+b, onde r e b são os parâmetros do filtro. A figura 3.4 mostra um filtro “Token Bucket”.
Dois outros parâmetros do balde de fichas também fazem parte da especificação de tráfego.
A unidade policiada mínima m e o tamanho de pacote máximo M. O parâmetro m especifica o tamanho mínimo do datagrama IP em bytes. Pacotes menores são contados como tendo tamanho m. O parâmetro M especifica o tamanho máximo dos pacotes em bytes que estão de acordo com as especificações de tráfego. Os elementos da rede precisam rejeitar uma requisição de serviço se o tamanho máximo de pacote requisitado for maior que o tamanho MTU do enlace. Resumindo, o filtro de balde de fichas é uma função de fiscalização que isola os pacotes que estão de acordo com as especificação de tráfego daqueles que não estão.
A especificação de requisição especifica a Qualidade de Serviço que o aplicativo quer requisitar para um fluxo específico. Essa informação depende do tipo de serviço e das necessidades do aplicativo que solicita a QoS. Ela pode consistir de uma largura de banda específica, um retardo máximo de pacote ou uma taxa de perda máxima de pacotes. Na implementação IS, a informação das especificações de tráfego e de requisição são usadas no programador de pacotes.

Serviço de carga controlada
O serviço de carga controlada tem a intenção de suportara classe de aplicativos que são altamente sensíveis às condições de sobrecarga na Internet, tal como ocorre com os aplicativos de multimídia. Esses aplicativos funcionam bem em redes não carregadas, mas degradam rapidamente em condições sobrecarregadas. Se um aplicativo usar o serviço de carga controlada, o desempenho de um fluxo de dados específico não irá degradar caso a carga da rede aumente.
O serviço de carga controlada oferece somente um nível de serviço que é intencionalmente mínimo. Não há recursos opcionais ou outras capacidades na especificação. O serviço oferece somente uma única função. Ele aproxima o serviço de melhor-tentativa em redes levemente carregadas. Isso significa que os aplicativos que fazem reserva de QoS usando os serviços de carga controlada recebem um serviço equivalente bem próximo ao serviço fornecido por um tráfego de melhor tentativa não controlado em condições de sobrecarga leve. Nesse contexto, condições levemente carregadas significam que um percentual alto de pacotes transmitidos será entregue com sucesso ao destino, e o retardo de trânsito de um percentual alto de pacotes entregues não irá exceder muito o retardo mínimo de trânsito.
Cada roteador em uma rede que aceita pedidos de serviços de carga controlada precisa garantir que uma largura de banda adequada e os recursos de processamento de pacotes estejam disponíveis para processar a solicitações de reservas de QoS. Isso pode ser realizado com o controle de admissão ativo. Antes que um roteador aceite uma nova reserva de QoS, representada pela especificação de tráfego, ele precisa considerar todos os recursos importantes, tais como largura de banda de enlaces, espaço de buffer do roteador de swicth e a capacidade computacional de encaminhamento de pacotes .
A classe de serviço de carga controlada não aceita ou não faz uso de valores-alvo específicos para parâmetros de controle como largura de banda, retardo ou perda.
Aplicativos que usam os serviços de carga controlada precisam suportar e ser a prova de perdas e retardos de pacotes.
As reservas de QoS usando os serviços de carga controlada precisam fornecer uma especificação de tráfego que consista dos parâmetros r e b do balde de fichas bem como a unidade m policiada mínima e o tamanho M de pacote máximo. Uma especificação de requisição não é necessária porque os serviços de carga controlada não oferecem funções para reservar uma largura de banda fixa ou garantir retardos de pacotes mínimos. Os serviços de carga controlada fornecem controle de QoS somente para tráfego que esteja de acordo com a especificação de tráfego fornecida no momento da montagem do pacote. Isso significa que as garantias do serviço aplicam-se somente aos pacotes que respeitam a regra do balde de fichas que diz que durante todos os períodos de tempo T, o montante de dados enviados não pode exceder rT=b.
Os serviços de carga controlada são projetados para aplicativos que podem tolerar uma quantia razoável de perda e retardo de pacotes, tal como software de aplicativos de áudio e videoconferência.

Serviço garantido
O modelo de serviço garantido propicia funções que garantem que os datagramas cheguem em um tempo de entrega garantido. Isso significa que cada pacote de um fluxo que está de acordo com as especificações de tráfego vai chegar pelo menos até o tempo de retardo máximo especificado no descritor do fluxo. O serviço garantido é usado em aplicativos que precisam de uma garantia que o datagrama vai chegar no receptor não depois de um certo tempo após ter sido transmitido da sua origem.

Por exemplo, os aplicativos multimídia em tempo real, como sistemas de transmissão de vídeo e áudio que usam tecnologias de sequenciamento de dados, não podem permitir que os datagramas cheguem depois do momento específico de sua exibição. Aplicativos que apresentam exigências críticas em tempo real, como a distribuição em tempo real de dados financeiros (preços compartilhados), também precisam de um serviço garantido. O modelo de serviço garantido não minimiza a variação (a diferença entre os retardos máximo e mínimo dos pacotes), mas ele controla o retardo máximo de enfileiramento.

O modelo de serviço garantido representa a extremidade final do controle de retardos em redes. Outros modelos de serviços que propiciam controle de retardos apresentam restrições muito mais tolerantes. Por isso, o modelo de serviço garantido é somente útil se for implementado em cada roteador ao longo do caminho de reserva.

O modelo de serviço garantido fornece aos aplicativos um controle considerável sobre seus retardos. È importante entender que o retardo em uma rede IP tem duas partes: um retardo de transmissão fixo e um retardo de variável de enfileiramento. O retardo fixo depende do caminho escolhido, o qual é determinado não por serviço garantido, mas pelo mecanismo de configurações. Todos os dados de pacotes em uma rede IP têm um retardo mínimo que é limitado pela velocidade da luz e pelo tempo de retorno dos pacotes de dados em todos os roteadores do caminho de roteamento. O retardo de enfileiramento é determinado pelo serviço garantido e é controlado pelos dois parâmetros já vistos: o balde de fichas (em particular, o tamanho b do balde) e a largura de banda R solicitada pela reserva. Esses parâmetros são usados para construir o modelo de fluido para o comportamento ponta a ponta de um fluxo que usa serviços garantidos.

O modelo de fluido especifica o serviço que seria propiciado por um enlace dedicado entre emissor e receptor que tenha a largura de banda R. No modelo de fluido, o serviço de fluxo é completamente independente do serviço de outros fluxos. A definição de serviço garantido conta com o resultado de que o retardo do fluido de um fluxo obedecendo um balde de fichas (r, b) e sendo servido por uma linha com largura de banda R é controlado por b/R enquanto R não for menor que r. O modelo de serviço garantido aproxima esse comportamento da taxa de serviço R, onde agora R é uma parte da largura de banda através do caminho de roteamento e não largura de banda de uma linha dedicada.

No modelo de serviço garantido, as especificações de tráfego e de requisição são usadas para preparar uma reserva de fluxo. A especificação de tráfego é representada pelos parâmetros do balde de fichas. A especificação de requisição contém o parâmetro R que especifica a largura de banda da reserva de fluxo. O modelo de serviço garantidos é definido na RFC 2212.

O RSVP

O modelo de Serviços Integrados usa o RSVP (Reservation Protocol – protocolo de reserva) para preparar e controlar as reservas de QoS. O RSVP é definido na RFC-2205 e tem o status de uma padrão proposto. Como o RSVP é um protocolo de controle da Internet e não um protocolo de roteamento, ele requer a existência de um protocolo de roteamento para operar. O protocolo RSVP executa baseado no IP e do UDP e precisa ser implementado em todos os roteadores no caminho de reserva. Os conceitos-chaves do RSVP são fluxos e reservas.

Uma reserva RSVP se aplica a um fluxo específico de pacotes de dados em um caminho específico através dos roteadores. Um fluxo é definido como um fluxo de dados distinguível de datagramas relacionados de um único emissor para um único receptor. Se o receptor for um endereço de multicast, um fluxo pode alcançar múltiplos receptores. O RSVP fornece o mesmo serviço para fluxos de unicast e de multicast. Cada fluxo é identificado no RSVP por seu endereço IP de destino e sua porta de destino. Todos os fluxos têm um descritor de fluxo dedicado que contém a QoS que um fluxo específico requer. O protocolo RSVP não entende o conteúdo do descritor de fluxo. Ele é transportado como um objeto opaco pelo RSVP e é entregue às funções de controle de tráfego do roteador (classificador e programador de pacotes) para processamento.

Como o RSVP é um protocolo simplex, as reservas são feitas somente em uma direção.

Nas conexões duplex, como conferências de vídeo e áudio em que cada emissor é também um receptor, torna-se necessário montar duas sessões RSVP para cada estação.

O protocolo RSVP é iniciado pelo receptor. Usando mensagens de sinalização RSVP, o emissor propicia uma QoS específica para o receptor que envia uma mensagem de reserva RSVP de volta com a QoS que deveria ser reservada para o fluxo do emissor para o receptor. Esse comportamento considera as exigências de QoS diferentes para receptor heterogêneos em grandes grupos de multicast. O emissor não precisa saber quais são as características de todos os possíveis receptores para estruturar as reservas.

Para estabelecer uma reserva com RSVP, os receptores enviam requisições de reservas para os emissores dependendo das capacidades de seus sistemas. Por exemplo, uma estação de trabalho rápida e um PC lento querem receber um vídeo MPEG de alta qualidade com 30 quadros por segundo que tem uma taxa de dados de 1,5 Mbps. A estação de trabalho tem capacidade suficiente para decodificar o vídeo, mas o PC só consegue decodificar 10 quadros por segundo. Se o servidor de vídeo enviar as mensagens para os dois receptores dizendo que ele pode enviar o fluxo de vídeo a 1,5 Mbps, a estação de trabalho pode retornar uma requisição de reserva para 1,5 Mbps. Mas o PC não precisa de toda a largura de banda para esse fluxo já que ele não conseguiria decodificar todos os quadros. Assim, o PC poderia enviar uma requisição de reserva para um fluxo com 10 quadros por segundo e 500 Kbps.

Operação do RSVP

Uma parte básica da reserva de um recurso é o caminho. Um caminho significa o lugar por onde vai passar um fluxo de pacotes através de roteadores diferentes a partir do emissor até chegar no receptor. Todos os pacotes que pertencem a um fluxo específico irão usar o mesmo caminho. Esse caminho é determinado se um emissor gerar mensagens de caminho RSVP que viajam no mesmo sentido do fluxo. Cada host emissor envia periodicamente uma mensagem de caminho para cada fluxo de dados que

ele origina. A mensagem de caminho contém informações de tráfego que descrevem a QoS para um fluxo específico.
Como o RSVP não faz o roteamento sozinho, ele usa a informação das tabelas de roteamento em cada roteador para encaminhar as mensagens RSVP.
Se a mensagem de caminho chegar no primeiro roteador RSVP, o roteador armazena o endereço IP do campo último salto da mensagem, que é o endereço do emissor. A seguir, o roteador insere seu próprio endereço IP no campo último salto, envia a mensagem de caminho para o roteador seguinte e o processo se repete até que a mensagem tenha chegado no receptor. Ao final desse processo, cada roteador saberá o endereço do roteador anterior e o caminho poderá ser acessado no sentido contrário. **A figura 3.5** mostra o processo de definição do caminho.

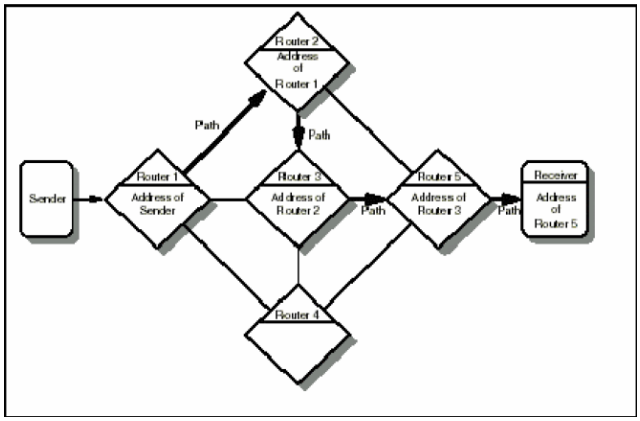


Figura – Processo de definição de um caminho RSVP

Os roteadores que receberam uma mensagem de caminho estão preparados para processar as reserva de recursos de um fluxo de dados. Todos os pacotes que pertencem a esse fluxo irão passar pelos mesmos roteadores: o caminho definido pelas mensagens de caminho.
O estado de um sistema após enviar as mensagens de caminho é o seguinte: todos os receptores sabem que um emissor pode fornecer uma QoS especial para um fluxo e todos os roteadores sabem sobre a possível reserva de recursos para esse fluxo.
Agora, se um receptor quiser reservar QoS para esse fluxo, ele envia uma mensagem de pedido de reserva. Essa mensagem de reserva contém a QoS solicitada por esse receptor para um fluxo específico e é representada pelas especificações de filtro e de fluxo que formam o descritor do fluxo. O receptor envia a mensagem de pedido de reserva para o último roteador no caminho com o endereço que ele recebeu da mensagem de caminho.
Como cada dispositivo capaz de RSVP sabe o endereço do dispositivo anterior do caminho, as mensagens de reserva percorrem o caminho no sentido oposto em direção ao emissor e estabelecem a reserva dos recurso em cada roteador. A figura abaixo mostra o fluxo das mensagens de reserva através dos roteadores.
Em cada nó, uma requisição de reserva inicia duas ações:

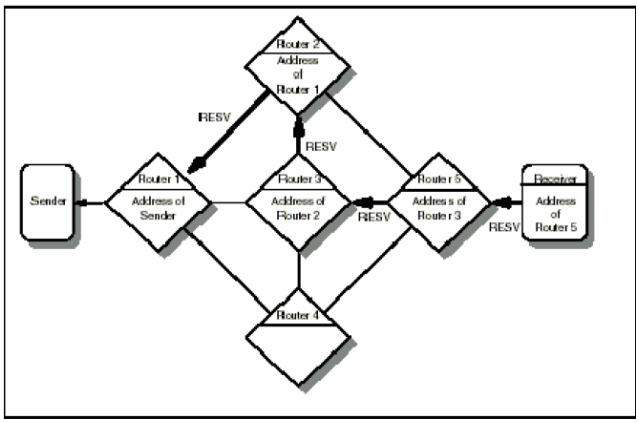


Figura 3.6 – Fluxo de mensagens de requisição de reserva RSVP

Reserva de QoS nesse enlace
O processo RSVP passa a requisição para o controle de admissão e para a instância de controle de plano de ação do nó. O controle de admissão verifica se o roteador tem os recursos necessários para estabelecer a nova reserva de QoS e o controle de plano de ação verifica se o aplicativo tem a autorização para fazer requisições de QoS. Se um desses testes falhar, a reserva será rejeitada e o processo RSVP retornará uma mensagem de erro ResvErr (erro na requisição de reserva) para o receptor apropriado. Se os dois testes forem bem-sucedidos, então o nó vai usar as informações da especificação de fluxo para preparar o programador de pacotes. Depois disso, o classificador de pacotes irá reconhecer os pacotes que pertencem a esse fluxo e o programador de pacotes irá obter a QoS desejada definida pela especificação de fluxo.

Encaminhamento da requisição de reserva
Após um teste de admissão e plano de ação bem-sucedido, uma requisição de reserva é propagada na direção do emissor. Em um ambiente de multicast, um receptor pode obter dados de vários emissores. O conjunto de hosts emissores para os quais uma certa requisição de reserva é propagado é chamado de alvo da requisição. A requisição de reserva que é encaminhada por um nó após uma reserva aprovada pode diferir de uma requisição que foi recebida do salto anterior no caminho em direção ao receptor. Uma razão possível disso é que o mecanismo de controle de tráfego pode modificar a especificação de fluxo a cada salto. Outro motivo mais importante é que em um ambiente de multicast, as reservas oriundas de ramos inferiores diferentes mas para o mesmo emissor são reunidas juntas à medida que percorrem o caminho upstream, na direção do emissor. Essa aglutinação é necessária para conservar recursos nos roteadores.
Uma requisição de reserva aprovada propaga-se na direção do emissor pela árvore de multicast até chegar em um ponto onde uma reserva existente seja igual ou maior que a que está sendo requisitada. Nesse ponto, a requisição que acaba de chegar é aglutinada com a reserva existente e não precisa mais ser passada adiante.
Se a requisição de reserva chegar no emissor, a reserva de QoS será estabelecida em cada roteador do caminho e o aplicativo poderá começar a enviar pacotes aos receptores. O classificador de pacotes e o programador de pacotes em

cada roteador garantem que os pacotes são encaminhados de acordo com a QoS requisitada.
Esse tipo de reserva é possível somente se todos os roteadores no caminho suportarem RSVP. Se apenas um roteador não suportar a reserva, o serviço não poderá ser garantido em todo o caminho por causa das restrições de "melhor tentativa" que se aplicam aos roteadores normais. Um roteador no caminho que não suporte RSVP representaria um gargalo para o fluxo.
Um receptor que origine uma requisição de reserva também pode requisitar uma mensagem de confirmação que indique que a requisição foi instalada na rede. O receptor inclui uma requisição de confirmação na mensagem de requisição de reserva e obtém uma mensagem de confirmação se a reserva tiver sido estabelecido com sucesso.
As reservas de recursos RSVP mantêm seus estados via software nos roteadores e hosts, o que significa que uma reserva será cancelada se um RSVP não enviar mensagens de atualização ao longo do caminho para uma reserva existente. Isso permite realizar mudanças de rota sem ocasionar sobrecarga do protocolo. As mensagens de caminho também precisam ser reenviadas porque os campos de estado do caminho nos roteadores serão reinicializados após um período de tempo.
Os estados de caminho e reserva também podem ser removidos por mensagens RVSP chamadas de teardown. Há dois tipos de mensagens "teardown":

Mensagens Path Tear
As mensagens "Path Tear" percorrem o caminho downstream a partir do ponto de iniciação de todos os receptores, removendo o estado do caminho bem como todos os estados de reservas dependentes em cada dispositivo capaz de RSVP.

Mensagens ResvTear
As mensagens "ResvTear" percorrem o caminho upstream a partir do ponto de iniciação de todos os emissores, removendo os estados de reservas em todos os roteadores e host.
Uma requisição de remoção de caminhos e reservas pode ser iniciada por emissores, receptores ou roteadores que notarem um tempo excedido de estado. Devido ao princípio de estado de software das reservas RSVP, não é realmente necessário remover explicitamente uma reserva antiga. Mesmo assim, é recomendado que todos os hosts de ponta enviem uma requisição de remoção se uma reserva existente não for mais necessária.

SERVIÇOS DIFERENCIADOS
O conceito de Serviços Diferenciados (DS) está atualmente sendo desenvolvido no grupo de trabalho DS da IETF. As especificações DS estão definidas em alguns esboços sobre a Internet IETF e não há nenhuma recomendação RFC disponível ainda. Este parágrafo fornecem uma visão geral sobre os fundamentos e as idéias sobre a diferenciação de serviços na Internet. Como o conceito ainda está sendo desenvolvido, algumas das especificações mencionadas neste livro podem ser alteradas na definição final dos serviços diferenciados.
O objetivo do desenvolvimento de DS é conseguir a possibilidade de fornecer classes diferenciadas de serviços para tráfego Internet e suportar vários tipos de aplicativos e requisitos específicos de negócios. DS oferece desempenho previsível (retardo, capacidade máxima, perda de pacotes etc..) para uma dada carga em um dado momento. A diferença entre os serviços integrados e os serviços diferenciados é que estes propiciam discriminação de serviços progressiva na Internet sem precisar de estados por fluxo e de sinalização a cada salto. Não é necessário realizar uma reserva de QoS em cada fluxo. Com DS, o tráfego da Internet é dividido em diferentes classes com diferentes requisitos de QoS.
Um componente central do DS é o SLA (Service Level Agreement – acordo de nível de serviço). O SLA é um contrato de serviço entre um cliente e um provedor de serviços que especifica os detalhes da classificação de tráfego e o serviço de encaminhamento correspondente que um cliente deve receber. Um cliente poderia ser uma organização de usuários ou outro domínio DS. O provedor de serviços precisa garantir que o tráfego de um cliente, com o qual ele tem um SLA, obtém a QoS contratada. Assim, a administração da rede do provedor de serviços precisa definir os planos de ação dos serviços apropriados e medir o desempenho da rede para garantir o desempenho de tráfego combinado.
Para distinguir os pacotes de dados de clientes diferentes em dispositivos de rede capazes de DS, os pacotes de IP são modificados em um campo específico. Um pequeno padrão de bits, chamado byte DS, cada pacote IP é usado para marcar os pacotes que irão receber um tratamento de encaminhamento particular em cada nó da rede. O byte DS usa o espaço do octeto TOS no cabeçalho IP Ipv4, "Formato de um Datagrama IP", e o octeto da classe de tráfego no cabeçalho de Ipv6. Todo tráfego da rede dentro de um domínio recebe um serviço que depende da classe de tráfego especificada no byte DS.

Para oferecer os serviços em conformidade com o SLA, os mecanismos a seguir precisam ser combinados em um rede:

- Configurar os bits do byte DS (octeto TOS) nas bordas da rede e nas fronteiras administrativos.
- Usar esses bits para determinar como os pacotes são tratados pelos roteadores dentro da rede.
- Condicionar os pacotes marcados nas fronteiras da rede de acordo com os requisitos de QoS de cada serviço.

A arquitetura DS atualmente definida propicia somente a diferenciação de serviços em um sentido e, portanto, é assimétrica. O desenvolvimento de uma arquitetura simétrica complementar é assunto atual de pesquisas. O parágrafo a seguir descreve a arquitetura com mais detalhes.

Arquitetura de serviços diferenciados
Diferente dos serviços integrados, as garantias de QoS nos serviços diferenciados são estáticas e permanecem por muito tempo nos roteadores. Isso significa que os aplicativos usando DS não precisam fazer reservas de QoS para pacotes de dados específicos. Todo o tráfego que passa por redes capazes de DS pode receber uma QoS

específica. Os pacotes de dados precisam ser marcados com o byte DS que é interpretado pelos roteadores da rede.

Uso de RSVP com serviços diferenciados

O protocolo RSVP, habilita os aplicativos a sinalizarem para uma rede as requisições por fluxo. Os parâmetros dos serviços integrados são usados para quantificar esse requisitos visando o controle de admissão. Mas o RSVP e os serviços integrados tem algumas limitações básicas que impedem a aplicação desses mecanismos na Internet como um todo:

- A dependência do RSVP dos estados por fluxo e dos processamentos por fluxos aumenta a preocupação com a capacidade de ampliação em redes grandes.
- Hoje em dia, um pequeno número de host gera sinalização RSVP. Embora espera-se que esse número cresça dramaticamente, muitos aplicativos podem nunca vir a gerar a sinalização RSVP.
- Muitos aplicativos exigem alguma forma de Qos, mas são incapazes de expressar essas necessidades usando o modelo IS.

Essas desvantagens podem ser superadas se os Serviços Integrados forem implementados somente em intranets e usarem Serviços Diferenciados na Internet como backbone.

A figura abaixo mostra uma estrutura de rede imaginária.

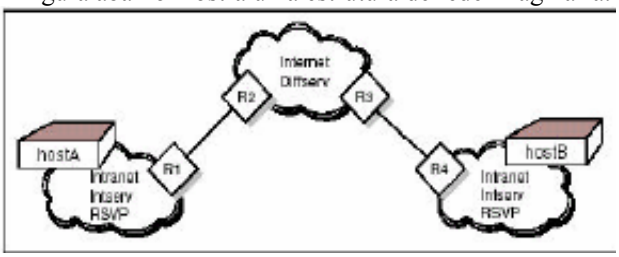


Figura – Uso de RSVP com serviços diferenciados

Duas intranets de clientes capazes de RSVP são conectadas ao backbone Internet DS. Os roteadores R2 e R3 são roteadores de fronteira que podem condicionar o tráfego de entrada e de saída nas interfaces da rede DS com as redes IS. Em nosso exemplo, os roteadores de fronteira não são necessários para executar RSVP. Espera-se que eles implementem as funções de fiscalização do roteador DS de ingresso. Deve haver um conjunto de serviços de ponta a ponta definidos na rede DS que permite o mapeamento das reservas de fluxo RSVP para uma classe de serviço DS apropriada. Os roteadores na rede DS precisam fornecer um conjunto de comportamento por salto, que propicia o serviço de uma conexão real ponto a ponto. Deve ser possível aos aplicativos RSVP chamar níveis de serviços específicos de ponta a ponta para seus fluxos de tráfego na rede DS. Nesse modelo, as intranets IS são clientes da Internet DS.

Os roteadores de borda R1 e R4 são roteadores especiais que trabalham tanto na região RSVP/IS como na região DS da rede. Esses roteadores podem ser vistos como divididos em duas metades. Uma metade suporta RSVP padrão e faz interface com as intranets. A outra metade suporta DS e faz interface com a Internet DS. A metade RSVP precisa ser, pelo menos, capaz parcialmente de RSVP. O Roteador precisa ser capaz de processar mensagens PATH e RESV mais não é preciso que suporte classificação de pacotes e armazenamento de estados RSVP. A metade DS do roteador propicia a interface com a função de controle de admissão na rede DS. Se o acordo de serviço entre as intranets IS e a Internet DS for estático, o serviço de controle de admissão pode ser uma tabela simples que especifica a QoS em cada nível de serviço. Se o acordo de serviço for dinâmico, o serviço de controle de admissão se comunica com as contrapartes dentro da rede DS para tomar decisões de controle de admissão com base na capacidade da rede.

Em nosso modelo, a sinalização RSVP é usada para propiciar controle de admissão para níveis de serviços específicos nas redes DS e IS. As mensagens de sinalização RSVP transportam uma descrição de QoS IS que especifica o tipo de serviço que deve ser propiciado nas regiões IS da rede. Na fronteira ente uma rede IS e uma rede DS os roteadores de borda correlacionam a QoS IS requisitadas com um nível de serviço DS apropriado. Depois disso, o roteador de borda pode prover controle de admissão para a rede DS, aceitando ou rejeitando a requisição de QoS com base na capacidade disponível no nível de serviço DS requisitado. Se uma mensagem de reserva RSVP oriunda da rede IS chegar em um roteador de borda, o descritor de fluxo RSVP será mapeado em um PHB que representa o nível de serviço correspondente na rede DS. O roteador de borda acrescenta o valor PHB à mensagem de reserva RSVP que é transportada para o host de envio. O host emissor então marca todos os pacotes de saída com esse valor de PHB. Esse método permite garantir uma QoS de ponta a ponta para aplicativos RSVP em intranets diferentes que usem a Internet DS como backbone.

RSVP E ROTEADORES (RESUMO DO RSVP)

O RSVP também pode ser executado em roteadores e funciona em conjunto com as solicitações sendo transmitidas por um aplicativo de rede. O RSVP é usado em roteadores para encaminhar solicitações de QoS para todas as estações ao longo do caminho ou caminhos de um determinado fluxo. Também cabe aos roteadores estabilizar e manter um estado de RSVP. Em outras palavras, se um aplicativo faz uma solicitação de RSVP, cada roteador deve encaminhá-lo para outro roteador na rota até a origem; sem , o caminho contrário, do receptor para o remetente.

Um processo de RSVP utiliza a tabele de rotas local para obter rotas.

A QoS é implementada por uma coleção de mecanismos conhecidos como controle de tráfego. Isso inclui três mecanismos.

Classificador de pacote: Determina a classificação de QoSs e possivelmente o roteador para cada pacote.

Controle de admissão: Determina se recursos estão disponíveis para aceitar ou rejeitar uma solicitação.

Programador de pacote: Arquiva a QoS prometida para cada interface de saída.

O slide mostra um diagrama para RSVP. Dois módulos dentro do RSVP conhecidos como *controle de admissão e controle de diretiva* são usados por uma solicitação de RSVP. O controle de admissão determina se o nó tem os

recursos disponíveis para aceitar a solicitação. O controle de diretiva determina os direitos de permissão do solicitante. O controle de diretiva determina os direitos de permissão do solicitante. Se uma dessas verificações falhar, o solicitante é descartado e a mensagem é enviada de volta para o solicitante (o aplicativo que fez a solicitação), indicando o tipo de falha. Se ambas as verificações forem removidas, os parâmetros serão definidos no classificador de pacote e no programador de pacote na esperança de obter os recursos exigidos pela solicitação.

Resumo do RSVP

As demandas de usuários individuais por um melhor serviço de IP estão levando à necessidade de algum tipo de reserva de largura de banda. A maioria de nós continua usando o telefone para fazer esse tipo de comparação. A Internet continua entregando qualquer tipo de dados com base na seguinte fórmula: primeiro que vem, primeiro que vai.

Os roteadores ainda soltam uma extraordinária quantidade de pacotes através da Internet, provocando retransmissões. Mais aplicativos estão sendo executados através da Internet diariamente. Aplicativos multimídia são os que exigem QoS somente porque os usuários assim o exigem. Esperamos isso devido às redes de TV a cabo e de telefone. O RSPV permitirá que isso exista, mas ele permanecerá restrito aos pockets de redes e não a toda a Internet. O RSVP colocará grandes demandas sobre os roteadores. Os roteadores atuais ainda têm de provar que podem manipular alguma coisa a mais do que simples encaminhamento de dados e mesmo isso não o estão fazendo bem. Roteadores mais rápidos estão chegando ao mercado e ajudarão a diminuir o problema.

A internet está se tornando canalizada, o que significa que haverá fluxos de dados percorrendo a Web os quais um usuário pode sintonizá-los. A questão que estou tentando levantar é que o QoS é composto de muitos fatores, e que o RSVP é apenas um deles. Não pensem que com a aplicação do RSVP todos os seus problemas aplicando outros fatores também, como compressão, filtros, priorização de protocolo, projeto de rede, OSPF e resumos de endereço, entre outras coisas. Uma coisa a mais: a multimídia realmente exige (para uma melhor operação) que o multicast seja habilitado. Apenas recentemente os ISPs começaram a tornar suas redes compatíveis com multicast (mesmo com toda a Internet sendo não multicast). O fluxo de dados em tempo real não é muito eficiente.

O RSVP é a primeira tentativa de fornecer algum tempo de Qualidade de Serviço com a base em uma necessidade do usuário por usuário.

Virtual LAN (VLANs)

Uma rede local virtual, normalmente denominada de **VLAN**, é uma rede logicamente independente. Várias VLAN's podem co-existir em um mesmo comutador (switch). O protocolo predominante é o IEEE 802.1Q. Antes da introdução do 802.1q, o protocolo ISL da Cisco, uma variante do IEEE 802.10, foi um dos vários protocolos proprietários. O ISL é desaprovado em favor do 802.1q.

As primeiras VLAN's geralmente eram configuradas para reduzir o tamanho do domínio de colisão em um segmento Ethernet muito extenso para melhorar o desempenho. Quando os switch's descartaram este problema (porque eles não têm um domínio de colisão), as atenções se voltaram para a redução do domínio de broadcast na camada MAC. Dependendo do tipo de configuração, os usuários ganham mobilidade física dentro da rede. Um outro propósito de uma rede virtual é restringir acesso a recursos de rede sem considerar a topologia da rede, porém este método é questionável.

Redes virtuais operam na camada 2 do modelo OSI. No entanto, uma VLAN geralmente é configurada para mapear diretamente uma rede ou sub-rede IP, o que dá a impressão que a camada 3 está envolvida.

Enlaces switch-a-switch e switch-a-roteador são chamados de troncos. Um roteador ou switch de camada 3 serve como o backbone entre o tráfego que passa através de VLAN's diferentes.

Redes virtuais podem ser configuradas de várias formas;

- Nível do protocolo, IP, IPX, LAT, etc.
- Baseada no endereço MAC.
- Baseada na sub-rede IP.
- Baseada na porta, e portanto, baseada no mundo real, como em departamento de marketing versus finanças.

VLAN's podem ser estáticas, dinâmicas ou dependente da porta. Existem dois métodos de estabelecer uma VLAN: por marcação de quadro (frame-tagging) e por filtragem de quadro (frame-filtering). A marcação de quadro modifica a informação que está contida dentro do quadro da camada 2, de tal modo que os switch's podem encaminhar o tráfego da VLAN para as suas VLAN's de destino e voltar o quadro ao seu formato normal. A filtragem de quadro faz o switch procurar por um certo critério no quadro da camada 2 e usar este sistema de comparação para encaminhar o tráfego para sua VLAN e destino corretos.

Um dispositivo de camada 2 pode implementar VLAN's de três maneiras diferentes;

- VLAN's abertas (Open VLANs) têm um banco de dados de endereço MAC único para todas as VLAN's.
- VLAN's fechadas (Closed VLANs) têm um banco de dados de endereço MAC separado para cada VLAN.
- VLAN's de modo mixado (Mixed Mode VLANs) podem ser configuradas como aberta ou fechada por VLAN.

VLAN's fechadas geralmente são consideradas mais seguras que VLAN's abertas.

Em equipamentos da Cisco, o VTP (VLAN Trunking Protocol) possibilita domínios de VLAN, os quais podem ajudar em tarefas administrativas. o VTP também permite "expurgo", assim, o tráfego de uma VLAN específica é direcionado apenas aos switch's que têm portas naquela VLAN.

Vantagens das Redes VLANs

- **Controle do tráfego broadcast**

As VLANs apresentam um desempenho superior as tradicionais redes locais, principalmente devido ao controle do tráfego broadcast**.**

Tempestades de quadros broadcast (*broadcast storms*) podem ser causadas por mal funcionamento de placas de interface de rede, conexões de cabos mal feitas e aplicações ou protocolos que geram este tipo de trafégo, entre outros.

Em redes onde o tráfego broadcast é responsável por grande parte do trafégo total, as VLANs reduzem o número de pacotes para endereços desnecessários, aumentando a capacidade de toda a rede.

De um outro ponto de vista, em uma rede local segmentada, os domínios de broadcast são menores. Isto porque cada segmento possui um menor número de dispositivos conectados, comparado ao existente na rede sem segmetação. Com isso, trafegam menos quadros broadcast tanto em cada segmento, quanto em toda rede.

- **Segmentação lógica da rede**

Como visto anteriormente, redes virtuais podem ser criadas com base na organização setorial de uma empresa. Cada VLAN pode ser associada a um departamento ou grupo de trabalho, mesmo que seus membros estejam fisicamente distantes. Isto proporciona uma segmentação lógica da rede .

- **Redução de custos e facilidade de gerenciamento**

Grande parte do custo de uma rede se deve ao fato da inclusão e da movimentação de usuários da mesma (mais detalhes em [3]). Cada vez que um usuário se movimenta é necessário um novo cabeamento, um novo endereçamento para estação de trabalho e uma nova configuração de repetidores e roteadores.

Em uma VLAN, a adição e movimentação de usuários pode ser feita remotamente pelo administrador da rede (da sua própria estação), sem a necessidade de modificações físicas, proporcionando uma alta flexibilidade.

- **Independência da topologia física**

VLANs proporcionam independência da topologia física da rede, permitindo que grupos de trabalho, fisicamente diversos, possam ser conectados logicamente a um único domínio broadcast.

- **Maior Segurança**

O tráfego em uma VLAN não pode ser "escutado" por membros de outra rede virtual, já que estas não se comunicam sem que haja um dispositivo de rede desempenhando a função de roteador entre elas. Desta forma, o acesso a servidores que não estejam na mesma VLAN é restrito, criando assim "*domínios de segurança no acesso a recursos*"

As redes locais virtuais limitam o tráfego a domínios específicos proporcionando mais segurança a estes

Tipos de VLANs

Quanto a forma de identificação dos seus membros, as redes locais virtuais podem ser classificadas em:

VLANs baseadas em:

- **Portas: camada 1**

Os membros de uma VLAN podem ser definidos de acordo com as portas da ponte/comutador utilizado. Por exemplo, em um comutador com dez portas, as portas 1, 2, 3 e 8 pertencem a VLAN 0. Já as portas 4, 9 e 10 fazem parte da VLAN 1. As demais pertencem a VLAN 2, como visto na figura 2

Portas	1	2	3	4	5	6	7	8	9	10
VLAN	0	0	0	1	2	2	2	0	1	1

Figura 2 - Associação de portas a diferentes VLANs

- **Endereço MAC (*Media Access Control*): camada 2**

Neste caso os membros da rede virtual são identificados pelo endereço MAC (*Media Access Control*) da estação de trabalho. O comutador reconhece o endereço MAC pertencente a cada VLAN. A associação entre endereços MAC e VLANS é exemplificado na figura 3

Endereço MAC	1212389145121	5043834758445	6673573385843
VLAN	0	1	1

Figura 3 - Associação de endereços MAC a diferentes VLANs

Quando uma estação de trabalho é movida, não é necessário reconfigurá-la para que esta continue pertencendo a mesma VLAN, já que o endereço MAC faz parte da sua placa de interface de rede. Isto é uma vantagem em relação as VLANs baseadas em portas, onde a tabela de membros tem de ser reconfigurada.

O grande problema deste método é que um membro de uma VLAN deve ser inicialmente especificado, obrigatoriamente. Em redes com milhares de usuários isto não é uma tarefa simples.

- **Protocolo: camada 2**

Os membros de uma VLAN camada 2 também podem ser identificados de acordo com o campo "tipo de protocolo" encontrado no cabeçalho da camada 2, como visto na figura 4

Protocolo	IP	IPX	NetBios
VLAN	0	0	1

Figura 4 - Associação de protocolos a diferentes VLANs

- **Endereço IP (*Internet Protocol*): camada 3**

Neste método os mebros pertencentes a uma VLAN são determinados pelo cabeçalho da camada 3. O endereço IP pode ser usado nesta classificação.

Endereço IP	146.164.69.2	146.164.69.28	146.164.69.10
VLAN	1	0	1

Figura 5 - Associação de endereço IP a diferentes VLANs

Embora um membro seja identificado por uma informação da camada 3, este processo não é realizado pelo roteador e também não há nenhuma relação com o roteamento nesta rede. Neste método, o endereço IP é usado somente como um mapeamento para determinar os usuários de uma VLAN.

Em VLANs camada 3, os usuários podem mover suas estações de trabalho sem reconfigurar os seus endereços de rede. O único problema é que geralmente o tempo para o encaminhamento de pacotes usando informações da camada 3 é maior do que utilizando o endereço MAC.

- **Camadas superiores**

Também é possível definir os membros de uma VLAN de acordo com aplicações ou serviços, ou uma combinação destes. Por exemplo, aplicações FTP (*File Transfer Protocol*) podem ser executadas em uma VLAN e aplicações telnet em outra.

Obs.: O padrão IEEE 802.1Q define somente VLANs das camadas 1 e 2. As demais são soluções proprietárias

Quando um dispositivo de rede (ponte, comutador), com suporte ao padrão IEEE 802.1Q, recebe quadros vindos de uma estação de trabalho, ele os rotula, marca. Este rótulo (*tag*), chamado de identificador VLAN (VID), indica a rede virtual de onde vem o quadro. Este processo é chamado de marcação explícita (*explicit tagging*).

Também é possível determinar a qual VLAN o quadro recebido pertence utilizando a marcação implícita (*implicit tagging*). Neste procedimento o quadro não é rotulado, mas VLAN de origem do quadro é identificada por outro tipo de informação, como por exemplo a porta onde o quadro chegou.

A marcação pode ser baseada na porta de onde veio o quadro, no campo do endereço MAC (*Media Access Control*) da fonte, no endereço de rede de origem ou algum outro campo ou combinação destes. As VLANs podem ser classificadas de acordo com o método utilizado.

Para ser capaz de rotular um quadro, utilizando qualquer um dos métodos citados anteriormente, o dispositivo de rede deve manter atualizado uma base de dados contendo um mapeamento entre VLANs e de onde e qual o campo é utilizado na marcação. Este banco de informações é chamado *filtering database* e deve ser o mesmo em todos os equipamentos.

O comutador, ou ponte, determina para onde deve ir o quadro como numa LAN. Uma vez indicado o destino do quadro, também é necessário determinar se o identificador VLAN deve ser adicionado ao quadro e enviado.

Caso o destino do quadro seja um dispositvo com suporte a VLANs (VLAN-*aware*) o identificador VID é adicionado. Entretanto, se o destinatário não suporta o padrão IEEE 802.1Q (VLAN-*unaware*), o dispositvo envia o quadro sem VID.

Para entender como funciona uma rede local virtual é necessário conhecer os seus tipos, as formas de conexão entre seus dispositvos, a base da dados utilizada para enviar corretamente os quadros a VLAN de destino (*filtering database*) e o processo de marcação, utilizado para identificar a VLAN originária do quadro.

De forma simplificada o funcionamento é ilustrado na figura 5.

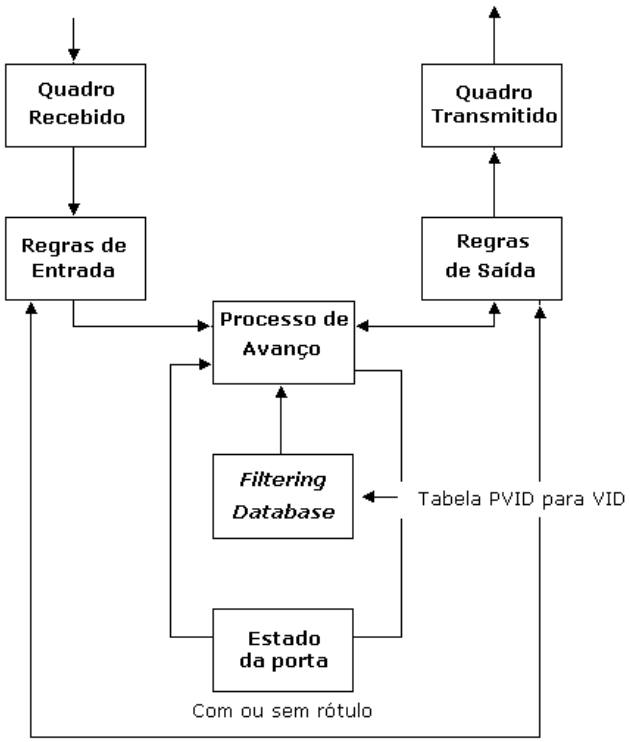


Figura 5 - O encaminhamento de pacotes para o padrão IEEE 802.1Q

As decisões sobre o encaminhamento dos quadros são baseadas nas três regras seguintes, considerando uma implementação baseada em portas (mais detalhes em "Classificação"):

- **Regras de Entrada (*Ingress Rules*)**, utilizadas para determinar a quais VLANs pertencem os quadros recebidos.
- **Regras de Encaminhamento entre Portas**, decidem se o quadro deve ser filtrado ou encaminhado.
- **Regras de Saída (*Egress Rules*)**, determinam se o quadro deve ser enviado com ou sem rótulo.

Classificação dos Quadros

As redes locais virtuais lidam com três tipos básicos de quadros:

- **Quadros sem rótulo (*Untagged frames*)**
- **Quadros com rótulo de prioridade (*Priority-tagged frames*)**
- **Quadros com rótulo VLAN (VLAN-*tagged frames*)**

Um quadro sem rótulo ou com rótulo de prioridade não carrega nenhuma identificação de qual VLAN veio. Tais quadros são classificados como vindos de uma VLAN particular baseado em parâmetros associados a porta receptora, ou, em soluções proprietárias, baseado no conteúdo do quadro (endereço MAC, identidficador de protocolo da camada 3, etc.).

É importante observar que para o propósito de indentifição de uma VLAN, os quadros com rótulo de prioridade são tratados igualmente aos sem rótulo. A prioridade é tratada por outro padrão, o IEEE 802.1p.

Um quadro com rótulo VLAN carrega um identificação explícita da sua VLAN de origem (VID), ou seja, ele possui em seu cabeçalho um rótulo contendo um campo VID não-nulo. Tal quadro é classificado como originário de uma VLAN particular baseado no valor deste identificador. A presença de um VID não-nulo no cabeçalho do quadro significa que algum outro dispositivo, ou o gerador do quadro ou uma ponte (ou comutador) com suporte a VLAN, mapeou este quadro em uma VLAN e inseriu o identificador apropriado.

Para uma dada VLAN, todos os quadros transmitidos devem ser rotulados obrigatoriamente da mesma forma neste segmento. Eles tem de ser ou todos sem rótulo, ou todos com rótulo VLAN, possuindo o mesmo VID.

Em outras palavras, um dispositivo pode transmitir quadros sem rótulo para algumas VLANs e quadros rotulados (VID) para outras em um dado enlace, mas não pode transmitir os dois formatos para mesma VLAN.

Marcação de quadros (*tagging*)

É necessário que os quadros, ao serem enviados através da rede, possuam um meio de indicar a qual VLAN pertencem, de modo que a ponte encaminhe-os somente para as portas que também pertencem a esta rede virtual. Do contrário, os quadros são encaminhados para todas as portas. Isto é o que normalmente ocorre.

Esta informação é adicionada ao quadro na forma de um rótulo ou marcação (*tag*) em seu cabeçalho. Este rótulo permite especificar informações sobre a prioridade de um usuário, assim como indica o formato do endereço MAC (*Media Access Control*).

Como visto anteriormente, quadros que possuem rótulo são enviados através de enlaces híbridos e "troncos".

Existem dois formatos de rótulos:

- **Rótulo para o cabeçalho do quadro Ethernet (*Ethernet Frame Tag Header*)**

O rótulo para o quadro Ethernet consiste em uma identificação do protocolo (TPID - Tag Protocol Identifier) e uma informação de controlo (TCI - Tag Control Information), figura 6.

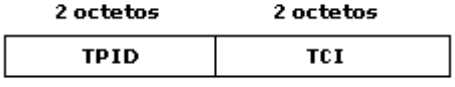


Figura 6 - Cabeçalho Ethernet com rótulo

- **Rótulo para o cabeçalho *Token Ring* e FDDI (*Fiber Distributed Data Interface*)**

O rótulo para o cabeçalho *token ring* e para o FDDI consiste de um campo TPID SNAP-codificado (SNAP-*enconded* TPID) e do campo TCI.

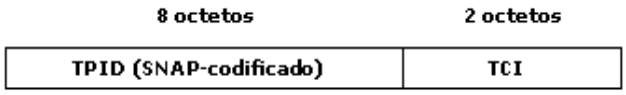


Figura 7- Cabeçalho *Token Ring* e FDDI com rótulo

O rótulo de identificação de protocolo indica que um rótulo de cabeçalho (*tag header*) vem a seguir. Já o TCI, figura 8, contém as informações sobre a prioridade do usuário, o formato canônico de indicação (CFI - *Canonical Format Indicator*), e o identificador VLAN (VID).

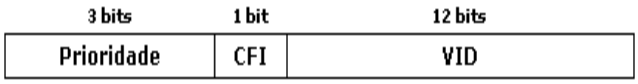


Figura 8 - Rótulo de informação de controle - TCI

O campo de prioridade possui 3 bits. Ele carrega informações de prioridade para serem codificadas no quadro. Existem oito níveis de prioridade. O nível zero é o de menor prioridade e o sete de maior prioridade. Maiores informações sobre prioridade podem ser obtidas no suplemento IEEE 802.1p, tema de outro trabalho desta disciplina.

O bit CFI é usado para indicar que todos os endereços MAC presentes no campo de dados MAC (MAC *data field*) estão na forma canônica. Este campo é interpretado de forma diferente de acordo com a tecnologia utilizada (Ethernet, *token ring*, FDDI).

O campo VID é utilizado para identificar, de forma única, a qual VLAN pertence o quadro. Podem existir um máximo de 4095 VLANs (2^{12} -1). O número zero é usado para indicar que não há um identificador VLAN, mas a informação sobre a prioridade está presente. Isto permite que a prioridade seja codificada em redes locais sem prioridade.

A inserção do rótulo no cabeçalho do quadro aumenta em quatro octetos o seu tamanho, no caso do Ethernet, e dez, no caso do *token ring*. Toda a informação contida no quadro original é retida.

Considerando como exemplo o quadro Ethernet, citado anteriormente, temos a seguinte situação, ilustrada na figura 9

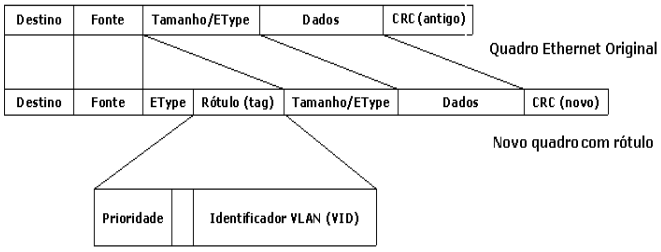


Figura 9 - Adicionando o rótulo 802.1Q ao cabeçalho Ethernet

O campo *EtherType* e o identificador VLAN são inseridos depois do endereço MAC da fonte, mas antes do campo *EtherType*/Tamanho ou Controle Lógico de Enlace (*Logical Link Control*). Como os quadros são agora mais longos, o CRC (*Cyclic Redundancy Check*) tem de ser recalculado

Tipos de Conexão

Dispositivos em uma rede local virtual podem ser conectados de três maneiras diferentes, levando-se em consideração se estem suportam ou não o padrão IEEE 802.1Q (VLAN-*aware* ou VLAN-*unaware*). São elas:

- **Enlace tronco (*Trunk Link*)**

Todos os dispositivos conectados a um enlace deste tipo, incluindo estações de trabalho, devem, obrigatoriamente, ter suporte à VLANs, isto é, serem dipositivos VLAN-*aware*. Todos os quadros em um *trunk link* tem de possuir um rótulo VLAN (mais detalhes em "classificação de quadros").

- **Enlace de Acesso (*Access Link*)**

Um enlace de acesso conecta um dispositivo sem suporte a VLAN a uma porta de uma ponte/comutador VLAN-*aware*. Todos os quadros neste tipo de enlace, obrigatoriamente, não devem possuir rótulo (mais detalhes em "classificação de quadros").

O dispositivo sem suporte pode ser um ou vários segmentos de uma rede local convencional contendo outros dispositivos também sem suporte ao IEEE 802.1Q.

- **Enlace Híbrido (*Hybrid Link*)**

Este é uma combinação dos dois enlaces anteriores. Em um enlace híbrido são conectados tanto dispositvos com suporte a VLANs, quanto os sem.

Num enlace desta natureza pode haver quadros com (*tagged frames*) e sem rótulo (*untagged frame*), mas todos

os quadros para uma VLAN específica tem de ser com rótulo VLAN ou sem rótulo.

Vale lembrar que para situações de identificação os quadros com rótulo de prioridade são tratados como "sem rótulo".

Base de Dados de Filtragem (*Filtering Database*)

As informações dos membros de uma VLAN são armazenadas em uma base de dados de filtragem (*Filtering Database*) que consiste de dois tipos de entrada: estáticas e dinâmicas.

Entradas Estáticas

Uma entrada estática é adicionada, modificada ou removida apenas por gerenciamento, ou seja, não são tratadas automaticamente. Existem dois tipos de entradas estáticas:

- **Entrada Estáticas de Filtragem**, que especificam para cada porta, se quadros devem ser enviados para um dado endereço MAC específico ou grupo de endereços e, em uma VLAN específica, devem ser encaminhados ou descartados, ou deve seguir a entrada dinâmica.
- **Entrada Estáticas de Registro**,que especificam se quadros a serem enviados para uma determinada VLAN serão rotulados ou não e quais portas são registradas para esta VLAN.

Entradas Dinâmicas

As entradas dinâmicas são aprendidas pelo dispositivo de rede e não podem ser criadas ou atualizadas por gerenciamento. O processo de aprendizagem (treinamento) observa a porta de onde o quadro, com um dado endereço fonte e um identificador VLAN (VID), foi recebido e atualiza a base de dados de filtragem (*filtering database*). A entrada só é atualizada se todas as seguintes condições forem satisfeitas:

- Esta porta permite aprendizado
- O endereço fonte (*source address*) é uma estação de trabalho válida e não um endereço de grupo (*group address*)
- Há espaço disponível na base de dados

As entradas são removidas da base de dados de acordo com o processo de "saída por envelhecimento" (*ageing out process*). Neste processo, depois de um certo tempo especificado por gerenciamento, as entradas permitem a reconfiguração automática da base de dados de filtragem, em caso de mudança na topologia da rede.

Existem três tipos de entradas dinâmicas:

- **Entradas Dinâmicas de Filtragem**, que especificam se quadros devem ser enviados para um endereço MAC específico e se devem ser encaminhados ou descartados em uma certa VLAN.
- **Entradas de Registro de Grupo**, que indicam, para cada porta, se quadros devem ser enviados para um endereço MAC de grupo e se devem ser encaminhados ou descartados em uma certa VLAN. Estas entradas são adicionadas e removidas mediante a utilização do Protocolo de Registro de Grupo Multidestinatário (GMRP - *Group Multicast Registration Protocol*). Isto permite que quadros multidestinatários (*multicast*) possam ser enviados em uma única VLAN sem afetar as demais.
- **Entradas Dinâmicas de Registro**, que especificam quais portas são registradas para uma VLAN específica. Estas entradas são adicionadas e removidas utilizando o Protocolo de Registro GARP VLAN (GVRP - GARP VLAN *Registration Protocol*), em que a sigla GARP significa Protocolo de Registro de Atributos Genéricos (*Generic Attribute Registration Protocol*).

O protocolo GVRP também é utilizado na comunicação entre pontes com suporte ao padrão IEEE 802.1Q.

Para que as redes locais virtuais encaminhem os pacotes para o destino correto, todas as pontes pertencentes a esta devem conter a mesma informação em suas respectivas base de dados. O protocolo GVRP permite que estações e pontes com suporte ao IEEE 802.1Q editem e revoguem membros de uma VLAN. As pontes também são responsáveis por registrar e propagar os membros de uma VLAN para todas as portas que participam da atual topologia desta. A topologia de uma rede é determinada quando as pontes são ligadas ou quando uma modificação no estado na topologia corrente é percebido.

A atual topologia da rede é determinada utilizando uma algoritmo "varredura" de árvore (*spanning tree algorithm*), o qual impede a formação de laços na rede destaivando as portas necessárias.

Uma vez obtida a atual topologia da rede, a qual contém diferentes VLANs, as pontes determinam a topologia corrente de cada rede virtual. Isto pode resultar em uma topologia diferente para cada VLAN ou uma comum para diversas destas. Em cada caso, a topologia da VLAN será um sub-conjunto da atual topologia da rede

Protocolos de Rede

Protocolo – É um conjunto de normas e regras que permite a comunicação entre computadores. O principal protocolo da internet , a base de todas as redes que é o protocolo TCP/IP.

A Arquitetura TCP/IP

A pilha, ou arquitetura TCP/IP foi originado da rede ARPANET, que foi criada como uma rede de pesquisa desenvolvida pelo Departamento de Defesa dos Estados Unidos, que pouco a pouco, centenas de universidades e repartições públicas foram sendo a ela conectadas através de linhas telefônicas privadas, resultando na atual rede mundial de computadores, a Internet.

O objetivo do TCP/IP era conectar várias redes locais, por isso o nome Internet, ou seja, inter redes ou entre redes. Após vários anos de trabalho de pesquisa, surgiu o modelo de referência TCP/IP, graças ao seus dois principais protocolos: o TCP, que significa Protocolo de Controle de Transporte; e o IP, que significa Protocolo Internet.

Na verdade, o acrônimo TCP/IP refere-se a uma grande família de protocolos que funciona em conjunto para permitir uma comunicação completa. Veremos mais adiante, que o conjunto de protocolos TCP/IP além de englobar os protocolos TCP e IP, também engloba outros protocolos, tais como ICMP (Internet Control Message Protocol) e o DNS (Domain Name Service), que permite a troca de mensagens de controle e a tradução de nomes (www.uol.com.br) em endereços numéricos (200.193.79.1), respectivamente.

As camadas do TCP/IP

O conjunto de camadas é conhecido como arquitetura de redes, e no caso do TCP/IP é assim dividido.

Camadas	Função
APLICAÇAO Protocolos: SMTP, TELNET, FTP, http, DNS, POP3, IMAP, NNTP	Reúne os protocolos de alto nível que fornecem serviços de comunicação ao usuário. Esses serviços são de acesso remoto (TELNET), correio eletrônico (SMTP, IMAP, POP3), transferência de arquivos (FTP), grupo de notícias (NNTP), abrir páginas da internet (http).
TRANSPORTE Protocolos: TCP, UDP	Reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e destino da comunicação, sem se preocupar com os elementos intermediários.
INTER-REDE Protocolos: IP, ICM, ARP, RARP	Responsável pela transferência de dados da máquina de origem à maquina destino, fazendo o roteamento e a comutação de pacotes.
INTERFACE DE REDE Protocolos: PPP, Ethernet, Token-Ring, FDDI, HDLC, SLIP, ATM.	É responsável pelo envio de datagramas construídos pela camada InterRede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-rede para um endereço físico ou lógico do nível de Rede.

Camada de Aplicação

A camada de aplicação reúne os protocolos que fornecem serviços de comunicação ao sistema ou ao usuário. Pode-se separar os protocolos de aplicação em protocolos de serviços básicos ou protocolos de serviços para o usuário:
Protocolos de serviços básicos, que fornecem serviços para atender as próprias necessidades do sistema de comunicação TCP/IP: DNS, BOOTP, DHCP
Protocolos de serviços para o usuário: FTP, HTTP, Telnet, SMTP, POP3, IMAP, TFTP, NFS, NIS, LPR, LPD, ICQ, RealAudio, Gopher, Archie, Finger, SNMP e outros

Camada de aplicação

Na Camada de Aplicação da Arquitetura TCP/IP temos os protocolos de alto nível:

SMTP (SIMPLE MAIL TRANSFER PROTOCOL) – Protocolo de envio de mensagens no Outlook Express. É necessário indicar um caminho de smtp para que as mensagens sejam levadas até um servidor. O programa padrão que cuida do gerenciamento das mensagens de correio eletrônico do seu computador é o *OUTLOOK EXPRESS.*

POP3 (POSTO OFFICE PROTOCOL) – Protocolo utilizado para o recebimento de mensagens, também é necessário indicar um caminho de *pop3* para a busca das mensagens no computador remoto. O protocolo pop3 só permite a leitura das mensagens se elas forem retiradas do servidor, ou seja, quando uma mensagem nova chega o pop3 faz a transferência das mensagens do servidor para o computador do usuário.

IMAP (INTERACTIVE MAIL ACCESS PROTOCOL) – Protocolo utilizado para a leituras das mensagens dentro do servidor sem a necessidade de transferência para o computador do usuário dessa maneira o usuário poderá acessar as mensagens de qualquer lugar.

FTP (FILE TRANSFER PROTOCOL) – Protocolo de transferência de arquvos e esta entre os mais antigos serviços da UNIX, sendo até hoje um dos protocolos de maior utilização na internet. Sua principal finalidade é transferir arquivos entre estações, tanto enviado quanto recebendo arquivos. De certa forma, o FTP compete com o serviço HTTP(web) em disponibilizar arquivos de acesso público na internet, porém possui funcionalidades mais peculiares que um servidor http, dentre as principais:

Comando de sistemas de arquivos - permite a execução de comandos remotos para manutenção de sistemas de arquivos.

Controle de permissões baseado em usuários – permite que usuário do sistema possam ser identificados.

Reinicio de transferências incompletas – isso é bastante útil para reiniciar um download de um arquivo muito longo por um cliente a partir do ponto em que foi finalizado por uma queda de conexão.

Compactação de arquivos sob demanda (on-the-fly) – suponha que tenha um diretório ou arquivo muito

grande no servidor remoto não compactados, com um tamanho que torna impossível baixa-los devido à sua baixa velocidade de acesso à internet.

HTTP (HYPER TEXT TRANSFER PROTOCOL) – é o protocolo padrão de transferência de conteúdo nos servidores Web, ou seja, é o protocolo que permite a visualização de páginas da web (Hipertextos) através de um programa de navegação ou "browser".

TELNET – é o protocolo que permite o acesso remoto a computadores.

DNS (DOMAIN NAME SERVICE) – A função do Servidor de Nomes de Domínio (DNS) transformar strings (nomes) para endereços IP. Primeiramente, os nomes e endereços eram armazenados automaticamente no seu computador local e por meio de arquivo texto. Tão logo uma rede ultrapassa alguns computadores, começam a surgir os problemas referentes a manter todos os endereços em todos os computadores. Faz sentido automatizar a manutenção da lista. Para resolver este problema foi criado o DNS que baseia-se em um computador que gerencia a lista e faz que os outros computadores o consultem para procurar endereços.

Camada de Transporte

Esta camada reúne os protocolos que realizam as funções de transporte de dados fim-a-fim, ou seja, considerando apenas a origem e o destino da comunicação, sem se preocupar com os elementos intermediários. A camada de transporte possui dois protocolos que são o UDP (User Datagram Protocol) e TCP (Transmission Control Protocol).

TCP (TRANSFER CONTROL PROTOCOL) – o Protocolo de Controle de Transmissão tem como objetivo controlar os dados quando estão em trafego, de forma que todos dados enviados de uma máquina deve ser divididos em pacotes pelo emissor, podendo trafegar por caminhos distintos e, finalmente, serem remontados corretamente pelo receptor. O protocolo também cuida da perda de pacotes no trajeto entre um ponto e outro, solicitando a retransmissão do pacote ao remetente. Toda vez que um pacote é enviado na rede, o protocolo TCP cuida das confirmações de recebimento. Portanto, é dito que o protocolo TCP constrói um serviço confiável. Outra característica importante do TCP é o controle de fluxo. Ao enviar dados na rede, a parte receptora indica à parte transmissora a quantidade de bytes que podem ser recebidos após os últimos dados recebidos, assim evita-se ultrapassar o limite da capacidade do *buffer* da máquina receptora.

O protocolo TCP realiza, além da multiplexação, uma série de funções para tornar a comunicação entre origem e destino mais confiável. São responsabilidades do protocolo TCP: o controle de fluxo, o controle de erro, a sequenciação e a multiplexação de mensagens.

A camada de transporte oferece para o nível de aplicação um conjunto de funções e procedimentos para acesso ao sistema de comunicação de modo a permitir a criação e a utilização de aplicações de forma independente da implementação. Desta forma, as interfaces socket ou TLI (ambiente Unix) e Winsock (ambiente Windows) fornecem um conjunto de funções-padrão para permitir que as aplicações possam ser desenvolvidas independentemente do sistema operacional no qual rodarão.

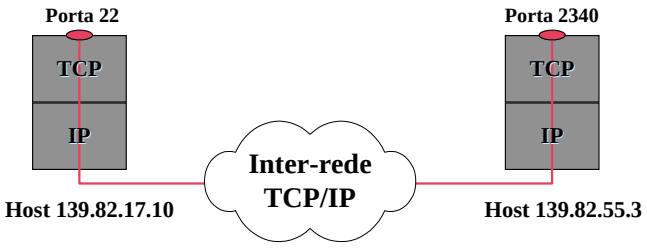
Resumindo, as principais características do TCP são:

- Controle de Fluxo e Erro fim-a-fim
- Serviço confiável de transferência de dados
- Comunicação full-duplex fim-a-fim
- A aplicação basta enviar um fluxo de bytes
- Desassociação entre qtd. de dados enviados pela aplicação e pela camada TCP
- Ordenação de mensagens
- Multiplexação de IP, através de várias portas
- Opção de envio de dados urgentes

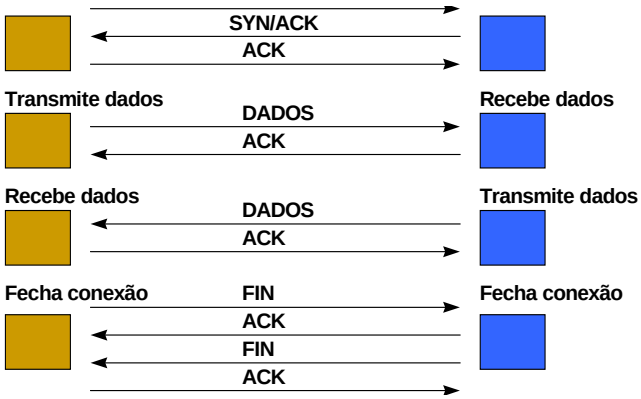
Algumas portas usadas pelo TCP para a sua comunicação.

PORTA	USO
11	Systat
15	Netstat
20	FTP (Dados)
21	FTP (Controle)
23	Telnet
25	SMTP
43	Whois
79	Finger
80	HTTP

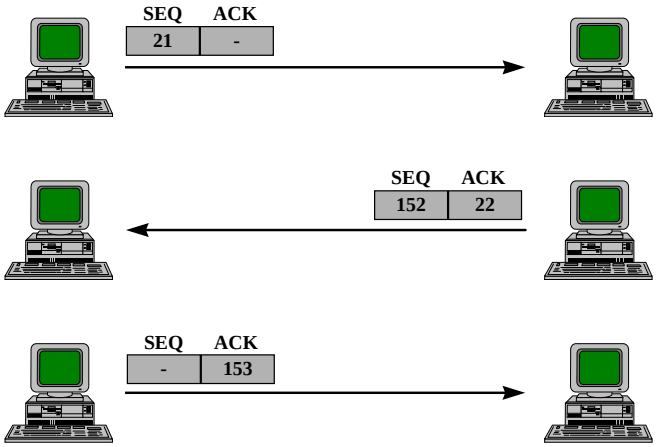
A conexão TCP é ilustrada na figura abaixo:



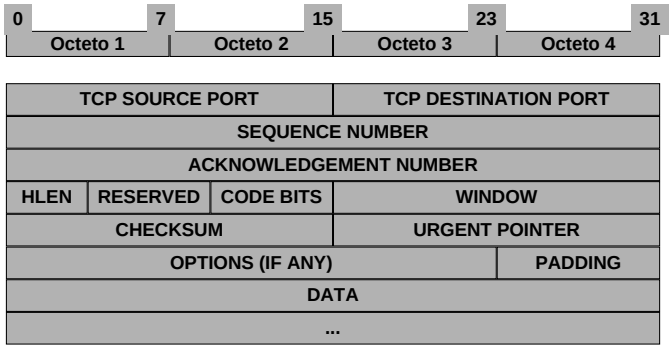
Uma conexão TCP é formada por três fases: o estabelecimento de conexão, a troca de dados e o finalização da conexão, conforme ilustrado na figura abaixo:



A fase inicial de estabelecimento de conexão é formada de três mensagens, formando o three-way-handshaking, conforme a figura abaixo:



O pacote TCP é formado pela mensagem mostrada abaixo:



Estes campos são definidos da seguinte forma:

TCP SOURCE PORT: Porta origem da mensagem
TCP DESTINATION PORT: Porta destino da mensagem
SEQUENCE NUMBER: número de sequência dos dados sendo transmitidos face ao conjunto total de dados já transmitidos. Este número indica a posição do primeiro byte de dados sendo transmitido em relação ao total de bytes já transmitidos nesta conexão. O primeiro número de sequência utilizado não é zero ou um, mas começa de um valor aleatório. Logo se um pacote está trasmitindo do 1234o. byte até o 2000o. byte de uma conexão e o SEQUENCE NUMBER inicial utilizado nesta conexão foi 10000, o campo SEQUENCE NUMBER conterá o valor 11234. O sequence number em um sentido da conexão (máquina A para B) é diferente do sequence number do sentido inverso, já que os dados transmitidos por um e outro lado são completamente distintos.
ACKNOWLEDGE NUMBER: número que significa o reconhecimento dos dados recebidos até então no sentido inverso. O ACK de um sentido é transmitido em piggy-backing no outro sentido. O ACK contém o número do próximo byte do fluxo de dados recebido, que a origem deste pacote espera receber da outra máquina. Este valor leva em consideração o número de SEQUENCE NUMBER inicial praticado pela outra máquina. O valor de ACK informa sempre o próximo byte ainda não recebido do conjunto contíguo de bytes recebidos do transmissor.

CODE BITS: São formados por seis bits, URG, ACK, PSH, RST, SYN e FIN, cuja utilização é mostrada abaixo:

- **URG**: bit de Urgência: significa que o segmento sendo carregado contém dados urgentes que devem ser lidos com prioridade pela aplicação. A aplicação origem é responsável por acionar este bit e fornecer o valor do URGENT POINTER que indica o fim dos dados urgentes. Um exemplo da utilização desta facilidade é o aborto de uma conexão (por exemplo por Control-C), que faz com que a aplicação destino examine logo o pacote até o fim da área de urgência, descubra que houve um Control-C e termine a conexão.
- **ACK**: bit de Reconhecimento: indica que o valor do campo de reconhecimento está carregando um reconhecimento válido.
- **PSH**: bit de PUSH: Este mecanismo que pode ser acionado pela aplicação informa ao TCP origem e destino que a aplicação solicita a transmissão rápida dos dados enviados, mesmo que ela contenha um número baixo de bytes, não preeenchendo o tamanho mínimo do buffer de transmissão.
- **RST**: bit de RESET: Informa o destino que a conexão foi abortada neste sentido pela origem
- **SYN**: bit de Sincronismo: é o bit que informa que este é um dos dois primeiros segmentos de estabelecimento da conexão.
- **FIN**: bit de Terminação: indica que este pacote é um dos dos pacotes de finalização da conexão

WINDOW: Este campo informa o tamanho disponível em bytes na janela de recepção da origem deste pacote. Por meio deste valor, o TCP pode realizar um controle adequando de fluxo para evitar a sobrecarga do receptor. Quando este valor é igual a zero, o transmissor não envia dados, esperando receber um pacote com WINDOW maior que zero. O transmissor sempre vai tentar transmitir a quantidade de dados disponíveis na janela de recepção sem aguardar um ACK. Enquanto não for recebido um reconhecimento dos dados transmitidos e o correspondente valor de WINDOW > 0, o transmissor não enviará dados.
OPTIONS: O campo de opções só possui uma única opção válida que é a negociação do MSS (Maximum Segment Size) que o TCP pode transmitir. O MSS é calculado através do MTU ou através do protocolo ICMP Path MTU Discovery.

UDP (USER DATAGRAM PROTOCOL) – protocolo de transporte mais simples, que não é orientado à conexão e não-confiável. É uma simples extensão do protocolo IP e foi desenvolvido para aplicações que não geram volume muito alto de tráfego na internet.
O protocolo UDP realiza apenas a multiplexação para que várias aplicações possam acessar o sistema de comunicação de forma coerente.

Camada de Inter-Rede, Rede ou Internet
Esta camada realiza a comunicação entre máquinas vizinhas através do protocolo IP. Para identificar cada máquina e a própria rede onde estas estão situadas, é definido um identificador, chamado endereço IP, que é independente de outras formas de endereçamento que

possam existir nos níveis inferiores. No caso de existir endereçamento nos níveis inferiores é realizado um mapeamento para possibilitar a conversão de um endereço IP em um endereço deste nível.

Os protocolos existentes nesta camada são:

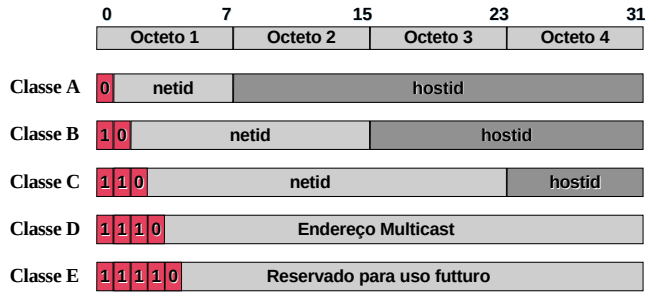
- Protocolo de transporte de dados: IP - Internet Protocol
- Protocolo de controle e erro: ICMP - Internet Control Message Protocol
- Protocolo de controle de grupo de endereços: IGMP - Internet Group Management Protocol
- Protocolos de controle de informações de roteamento

IP (INTERNET PROTOCOL) – o Protocolo Internet é a chave de interligação de redes que utilizam tecnologias e hardwares diferentes. Uma das características mais importantes do protocolo IP é a divisão da informação a ser transportada de uma ponto ao outro em fragmentos denominados datagramas. Todo datagrama é divido em cabeçalho e corpo. No cabeçalho encontram-se informações como: origem e destino do pacote, e informações específicas do protocolo pertinente a este pacote, já o corpo do datagrama é utilizado para armazenar os dados, ou seja, ao mandar um e-mail a concatenação do corpo dos datagramas no destino formará a mensagem original do e-mail enviada pela origem. A principal vantagem do IP reside no fato de transformar redes fisicamente separadas, com diferentes hardwares em uma rede funcionalmente homogênea. O protocolo IP resolve o problema da falta de espaço no *buffer* simplesmente descartando os pacotes, por isso diz-se que IP é um protocolo não confiável.
O protocolo IP realiza a função mais importante desta camada que é a própria comunicação inter-redes. Para isto ele realiza a função de **roteamento** que consiste no transporte de mensagens entre redes e na decisão de qual rota uma mensagem deve seguir através da estrutura de rede para chegar ao destino.
O protocolo IP utiliza a própria estrutura de rede dos níveis inferiores para entregar uma mensagem destinada a uma máquina que está situada na mesma rede que a máquina origem. Por outro lado, para enviar mensagem para máquinas situadas em redes distintas, ele utiliza a função de roteamento IP. Isto ocorre através do envio da mensagem para uma máquina que executa a função de roteador. Esta, por sua vez, repassa a mensagem para o destino ou a repassa para outros roteadores até chegar no destino.

Endereços IP
Um endereço IP é um identificador único para certa interface de rede de uma máquina. Este endereço é formado por 32 bits (4 bytes) e possui uma porção de identificação da rede na qual a interface está conectada e outra para a identificação da máquina dentro daquela rede.
O endereço IP é representado pelos 4 bytes separados por "ponto" e representados por números decimais. Desta forma o endereço IP:

11010000 11110101 0011100 10100011
é representado por
208.245.28.63.

Como o endereço IP identifica tanto uma rede quanto a estação a que se refere, fica claro que o endereço possui uma parte para rede e outra para a estação. Desta forma, uma porção do endereço IP designa a rede na qual a estação está conectada, e outra porção identifica a estação dentro daquela rede.
Uma vez que o endereço IP tem tamanho fixo, uma das opções dos projetistas seria dividir o endereço IP em duas metades, dois bytes para identificar a rede e dois bytes para a estação. Entretanto isto traria inflexibilidade pois só poderiam ser endereçados 65536 redes, cada uma com 65536 estações. Uma rede que possuísse apenas 100 estações estaria utilizando um endereçamento de rede com capacidade de 65536 estações, o que também seria um desperdício.
A forma original de dividir o endereçamento IP em rede e estação, foi feita por meio de classes. Um endereçamento de classe A consiste em endereços que tem uma porção de identificação de rede de 1 byte e uma porção de identificação de máquina de 3 bytes. Desta forma, é possível endereçar até 256 redes com 2 elevado a 32 estações. Um endereçamento de classe B utiliza 2 bytes para rede e 2 bytes para estação, enquanto um endereço de classe C utiliza 3 bytes para rede e 1 byte para estação. Para permitir a distinção de uma classe de endereço para outra, utilizou-se os primeiros bits do primeiro byte para estabelecer a distinção (veja figura abaixo).
Nesta forma de divisão é possível acomodar um pequeno número de redes muito grandes (classe A) e um grande número de redes pequenas (classe C). Esta forma de divisão é histórica e não é mais empregada na Internet devido ao uso de uma variação que é a sub-rede, como será visto em seção adiante. Entretanto sua compreensão é importante para fins didáticos.
As classes originalmente utilizadas na Internet são A, B, C, D, E., conforme mostrado abaixo. A classe D é uma classe especial para identificar endereços de grupo (multicast) e a classe E é reservada.



A Classe A possui endereços suficientes para endereçar 128 redes diferentes com até 16.777.216 hosts (estações) cada uma.
A Classe B possui endereços suficientes para endereçar 16.384 redes diferentes com até 65.536 hosts cada uma.
A Classe C possui endereços suficientes para endereçar 2.097.152 redes diferentes com até 256 hosts cada uma.

As máquinas com mais de uma interface de rede (caso dos roteadores ou máquinas interligadas à mais de uma rede, mas que não efetuam a função de roteamento) possuem um endereço IP para cada uma, e podem ser identificados por qualquer um dos dois de modo independente. Um endereço IP identifica não uma máquina, mas uma conexão à rede.

Alguns endereços são reservados para funções especiais:

Endereço de Rede: Identifica a própria rede e não uma interface de rede específica, representado por todos os bits de hostid com o valor ZERO.

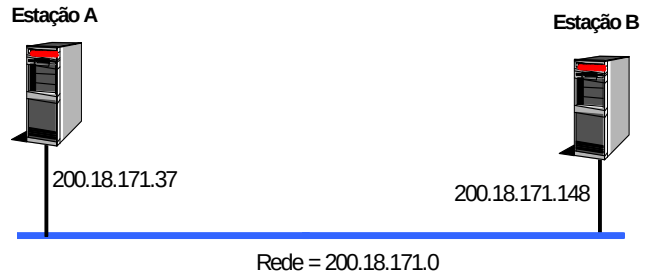
Endereço de Broadcast: Identifica todas as máquinas na rede específica, representado por todos os bits de hostid com o valor UM.

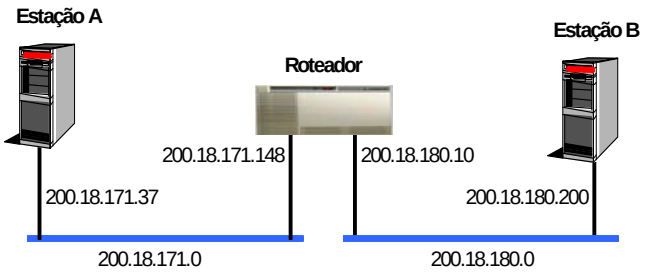
Desta forma, para cada rede A, B ou C, o primeiro endereço e o último são reservados e não podem ser usados por interfaces de rede.

Endereço de Broadcast Limitado: Identifica um broadcast na própria rede, sem especificar a que rede pertence. Representado por todos os bits do endereço iguais a UM = 255.255.255.255.

Endereço de Loopback: Identifica a própria máquina. Serve para enviar uma mensagem para a própria máquina rotear para ela mesma, ficando a mensagem no nível IP, sem ser enviada à rede. Este endereço é 127.0.0.1. Permite a comunicação inter-processos (entre aplicações) situados na mesma máquina.

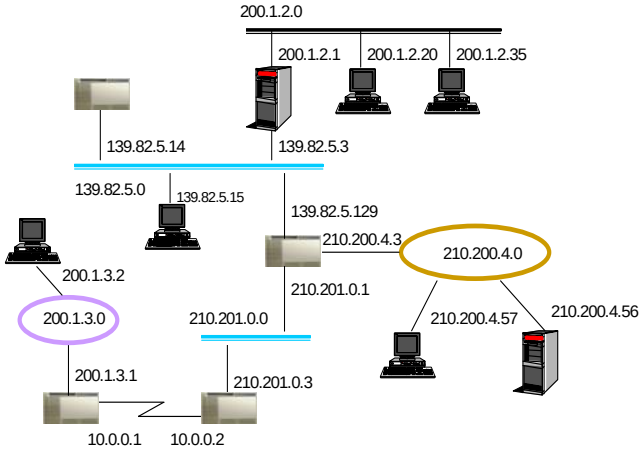
As figuras abaixo mostram exemplos de endereçamento de máquinas situadas na mesma rede e em redes diferentes. Pode ser observado que como o endereço começa por 200 (ou seja, os dois primeiros bits são 1 e o terceiro 0), eles são de classe C. Por isto, os três primeiros bytes do endereço identificam a rede. Como na primeira figura, ambas as estações tem o endereço começando por 200.18.171, elas estão na mesma rede. Na segunda figura, as estações estão em redes distintas e uma possível topologia é mostrada, onde um roteador interliga diretamente as duas redes.





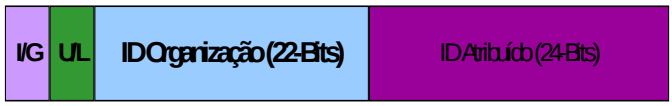
A figura abaixo ilustra um diagrama de rede com o endereçamento utilizado. Note que não há necessidade de correlação entre os endereços utilizados nas redes adjacentes. O mecanismo para que uma mensagem chegue na rede correta é o roteamento. Cada elemento conectando mais de uma rede realiza a função de roteamento IP, baseado em decisões de rotas. Note que mesmo os enlaces formados por ligações ponto-a-pontos são também redes distintas.

Neste diagrama existem 6 redes, identificadas por 200.1.2.0, 139.82.0.0, 210.200.4.0, 210.201.0.0, 10.0.0.0 e 200.1.3.0.



Mapeamento de endereços IP em endereços de rede

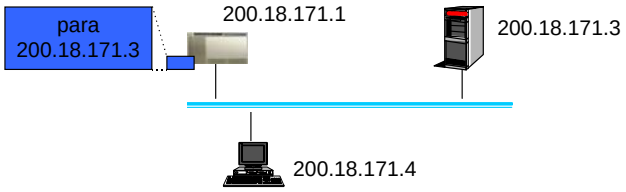
Os protocolos de rede compartilhada como Ethernet, Token-Ring e FDDI possuem um endereço próprio para identificar as diversas máquinas situadas na rede. Em Ethernet e Token-Ring o endereçamento utilizado é chamado endereço físico ou endereço MAC - Medium Access Control , formado por 6 bytes, conforme a figura abaixo:



Este tipo de endereçamento só é útil para identificar diversas máquinas, não possuindo nenhuma informação capaz de distinguir redes distintas. Para que uma máquina com protocolo IP envie um pacote para outra máquina situada na mesma rede, ela deve se basear no protocolo de rede local, já que é necessário saber o endereço físico. Como o protocolo IP só identifica uma máquina pelo endereço IP, deve haver um mapeamento entre o endereço IP e o endereço de rede MAC. Este mapeamento é realizado pelo protocolo ARP.

O mapeamento via protocolo ARP só é necessário em uma rede do tipo compartilhada como Ethernet, Token-Ring, FDDI, etc.. Em uma rede ponto-a-ponto como, por exemplo, um enlace serial, o protocolo ARP não é necessário, já que há somente um destino possível.

A figura abaixo mostra uma rede com 3 estações, onde uma máquina A com endereço IP 200.18.171.1 deseja enviar uma mensagem para a máquina B cujo endereço é 200.18.171.3. A mensagem a ser enviada é uma mensagem IP. No caso do exemplo abaixo, antes de efetivamente enviar a mensagem IP, a estação utilizará o protocolo ARP para determinar o endereço MAC da interface cujo endereço IP é o destino da mensagem.



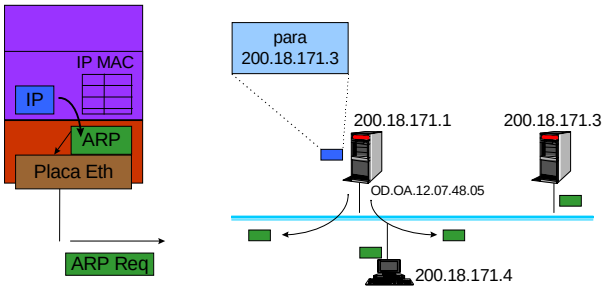
O funcionamento do protocolo ARP é descrito abaixo:

1. Estação A verifica que a máquina destino está na mesma rede local, determinado através dos endereços origem e destino e suas respectivas classes.

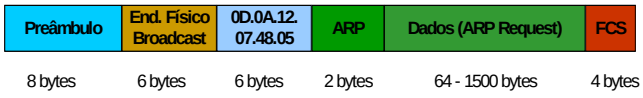
2. O protocolo IP da estação A verifica que ainda não possui um mapeamento do endereço MAC para o endereço IP da máquina destino.

3. O protocolo IP solicita ao protocolo que o endereço MAC necessário

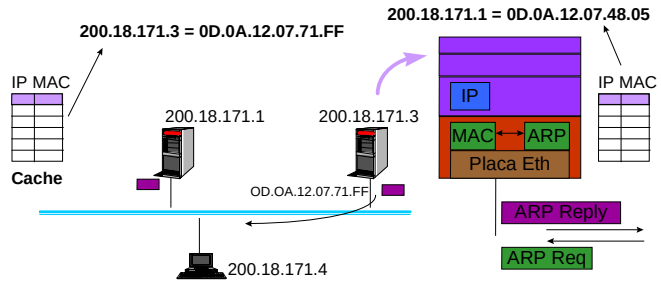
4. Protocolo ARP envia um pacote ARP (ARP Request) com o endereço MAC destino de broadcast (difusão para todas as máquinas)



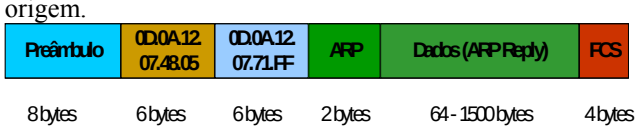
5. A mensagem ARP enviada é encapsulada em um pacote Ethernet conforme mostrado abaixo:



6. Todas as máquinas recebem o pacote ARP, mas somente aquela que possui o endereço IP especificado responde. A máquina B já instala na tabela ARP o mapeamento do endereço 200.18.171.1 para o endereço MAC de A.

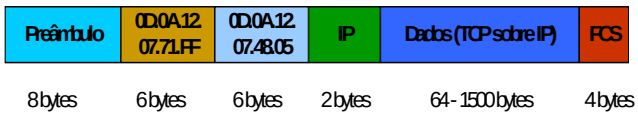


7. A resposta é enviada no pacote Ethernet, encapsulado conforme mostrado abaixo, através de uma mensagem ARP Reply endereçado diretamente para a máquina origem.

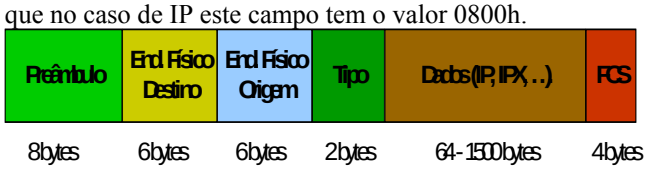


8. A máquina A recebe o pacote e coloca um mapeamento do endereço IP de B e seu endereço MAC respectivo. Esta informação residirá em uma tabela que persistirá durante um certo tempo.

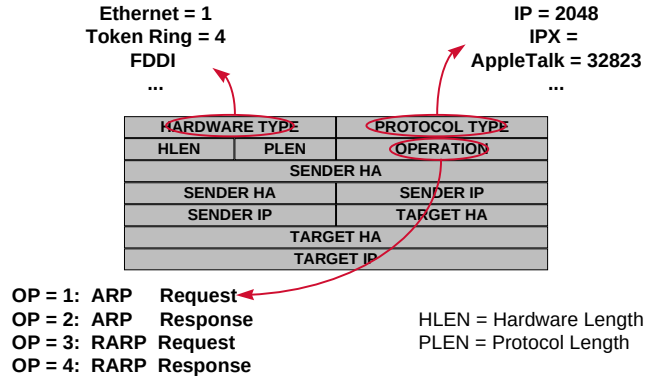
9. Finalmente a máquina A transmite o pacote IP inicial, após saber o endereço MAC da estação destino.



Os protocolos de nível de Rede como Ethernet possuem um identificador para determinar o tipo do protocolo que está sendo carregado no seu campo de dados. Um pacote Ethernet pode, por exemplo, carregar os protocolos ARP, IP, RARP, IPX, Netbios e outros. A figura abaixo mostra o formato do quadro Ethernet. Note que o campo protocolo, de 2 bytes de tamanho identifica o protocolo sendo carregado no campo de dados. No caso de transporte de um pacote ARP, o valor é 0806h (hexadecimal), enquanto que no caso de IP este campo tem o valor 0800h.



O protocolo ARP possui dois pacotes, um REQUEST e um REPLY, com o formato abaixo. No REQUEST, são preenchidos todos os dados exceto o endereço MAC do TARGET. No REPLY este campo é completado.



HARDWARE TYPE identifica o hardware (Ethernet, Token-Ring , FDDI, etc) utilizado, que pode variar o tamanho do endereço MAC.
PROTOCOL TYPE identifica o protocolo sendo mapeado (IP, IPX, etc,) que pode variar o tipo do endereço usado.
OPERATION identifica o tipo da operação, sendo
1 = ARP Request, 2 = ARP Reply, 3 = RARP Request, 4 = RARP Reply

Roteamento IP

O destino de um mensagem IP sendo enviado por uma máquina pode ser a própria estação, uma estação situada

na mesma rede ou uma estação situada numa rede diferente. No primeiro caso, o pacote é enviado ao nível IP que o retorna para os níveis superiores. No segundo caso, é realizado o mapeamento por meio de ARP e a mensagem é enviada por meio do protocolo de rede.
Quando uma estação ou roteador deve enviar um pacote para outra rede, o protocolo IP deve enviá-lo para um roteador situado na mesma rede. O roteador por sua vez irá enviar o pacote para outro roteador, na mesma rede que este e assim sucessivamente até que o pacote chegue ao destino final. Este tipo de roteamento é chamado de Next-Hop Routing, já que um pacote é sempre enviado para o próximo roteador no caminho.
Neste tipo de roteamento, não há necessidade de que um roteador conheça a rota completa até o destino. Cada roteador deve conhecer apenas o próximo roteador para o qual deve enviar a mensagem. Esta decisão é chamada de decisão de roteamento. Uma máquina situado em uma rede que tenha mais de um roteador deve também tomar uma decisão de roteamento para decidir para qual roteador deve enviar o pacote IP.
Quando uma estação deve enviar uma mensagem IP para outra rede, ela deve seguir os seguintes passos:

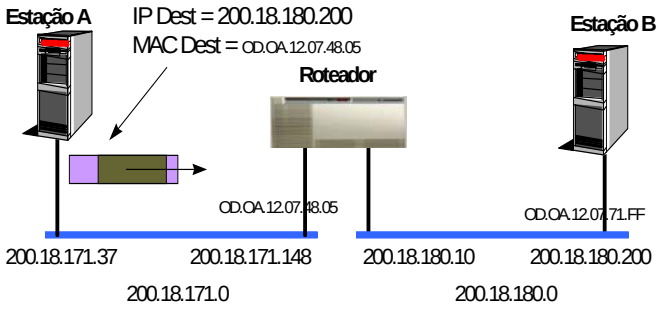
1. Determinar que a estação destino está em outra rede e por isto deve-se enviar a mensagem para um roteador

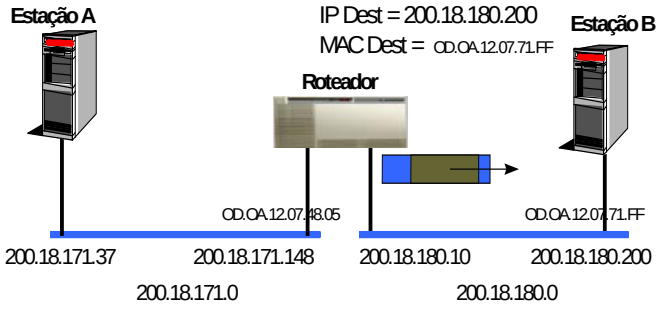
2. Determinar, através da tabela de rotas da máquina origem, qual roteador é o correto para se enviar a mensagem

3. Descobrir, através do protocolo ARP, qual o endereço MAC do roteador

4. Enviar a mensagem IP com o endereço de nível de rede apontado para o roteador e o endereço IP (na mensagem IP) endereçado para a máquina destino.

Uma questão importante no pacote roteado consiste no fato de que o pacote a ser roteado é endereçado fisicamente ao roteador (endereço MAC), mas é endereçado logicamente (endereçamento IP) à máquina destino. Quando o roteador recebe um pacote que não é endereçado a ele, tenta roteá-lo.
A decisão de roteamento é baseada em uma tabela, chamada de tabela de rotas, que é parte integrante de qualquer protocolo IP. Esta tabela relaciona cada rede destino ao roteador para onde o pacote deve ser enviado para chegar a ela.
As figuras abaixo mostram o funcionamento do roteamento:





Nas figuras acima o roteamento é realizado somente por um roteador. Caso houvesse mais de um roteador a ser atravessado, o primeiro roteador procederia de forma idêntica à Estação A, ou seja determinaria a rota correta e enviaria a mensagem para o próximo roteador.
O Algoritmo de **Transmissão** de um pacote IP é descrito abaixo. A transmissão pode ser aplicada tanto a um host quanto a uma estação:
1. Datagrama pronto para ser transmitido
2. Caso:
 2.1 Endereço Destino == Endereço Transmissor
  2.1.1 Entrega datagrama pela interface loopback (127.0.0.1)
  2.2.2 Fim
 2.2 Endereço de rede do destino == endereço de rede local
  2.2.1 Descobre o endereço físico do destino (ARP)
  2.2.1 Transmite datagrama pela interface correta
  2.2.2 Fim
 2.3 Endereço de rede do destino != endereço de rede local
  2.3.1 Verifica tabela de rotas
  2.3.2 Descobre rota que se encaixa com a rede destino
  2.3.3 Descobre o endereço físico do gateway (ARP)
  2.3.4 Transmite o datagrama para o gateway
  2.3.5 Fim
3. Fim
O Algoritmo de **Recepção** de um pacote IP é descrito abaixo:
1. Datagrama recebido da camada intra-rede, defragmentado e testado
2. Caso:
 2.1 Endereço Destino = Endereço do Host, ou E.D. = outras interfaces do Host, ou E.D. = Broadcast
  2.1.1 Passa datagrama para níveis superiores -> FIM
 2.2 Caso:
  2.2.1 Máquina que recebeu não é roteador
   2.2.1.1 Descarta datagrama -> FIM
2.2.2 Máquina é roteador (possui mais de uma interface IP)
  2.2.2 Caso:
   2.2.2.1 Endereço IP destino = Rede IPcom interface direta
    2.2.2.1.1 Descobre o endereço físico do destino (ARP)
    2.2.2.1.2 Transmite datagrama pela interface respectiva -> FIM
   2.2.2.2 Caso Endereço de rede do destino endereço de rede local
    2.2.2.2.1 Verifica tabela de rotas

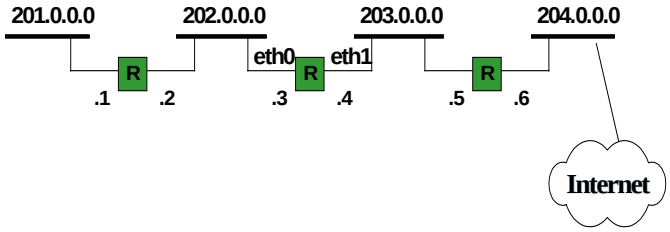
2.2.2.2.2 Descobre o endereço físico do gateway (ARP)

2.2.2.2.3 Transmite o datagrama para o gateway -> FIM

3. Fim

O exemplo abaixo ilustra uma estrutura de redes e a tabela de rotas dos roteadores. As tabelas de rotas de cada roteador são diferentes uma das outras. Note nestas tabela a existência de rotas diretas, que são informações redundantes para identificar a capacidade de acessar a própria rede na qual os roteadores estão conectados. Este tipo de rota apesar de parecer redundante é útil para mostrar de forma semelhante as rotas diretas para as redes conectadas diretamente no roteador.

Outra informação relevante é a existência de uma rota **default**. Esta rota é utilizada durante a decisão de roteamento no caso de não existir uma rota específica para a rede destino da mensagem IP. A rota default pode ser considerada como um resumo de diversas rotas encaminhadas pelo mesmo próximo roteador. Sem a utilização da rota default, a tabela de rotas deveria possuir uma linha para cada rede que pudesse ser endereçada. Em uma rede como a Internet isto seria completamente impossível.



A tabela de rotas para o roteador da esquerda é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
201.0.0.0	eth0 (rota direta)	0
202.0.0.0	eth1 (rota direta)	0
203.0.0.0	202.0.0.3	1
204.0.0.0	203.0.0.3	2
default	203.0.0.3	--

A tabela de rotas para o roteador central é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
202.0.0.0	eth0 (rota direta)	0
203.0.0.0	eth1 (rota direta)	0
201.0.0.0	202.0.0.2	1
204.0.0.0	203.0.0.5	1
default	203.0.0.5	--

A tabela de rotas para o roteador da direita é descrita abaixo:

Rede Destino	Roteador (Gateway)	Hops
203.0.0.0	eth0 (rota direta)	0
204.0.0.0	eth1 (rota direta)	0
202.0.0.0	203.0.0.4	1
201.0.0.0	203.0.0.4	1
default	204.0.0.7**	--

** Não mostrado na figura.

A rota default geralmente é representada nos sistemas operacionais como a rede 0.0.0.0

Roteamento estático x Roteamento dinâmico

A alimentação das informações na tabela de rotas pode ser de modo estático ou dinâmico ou ambos simultâneamente. Na alimentação estática, as rotas são preenchidas manualmente, geralmente pela configuração inicial da máquina. Na alimentação dinâmica, protocolos como RIP, RIP2, OSPF ou BGP4 são responsáveis pela aquisição de informações sobre a topologia da rede e a publicação de rotas na tabela de rotas dos roteadores envolvidos.

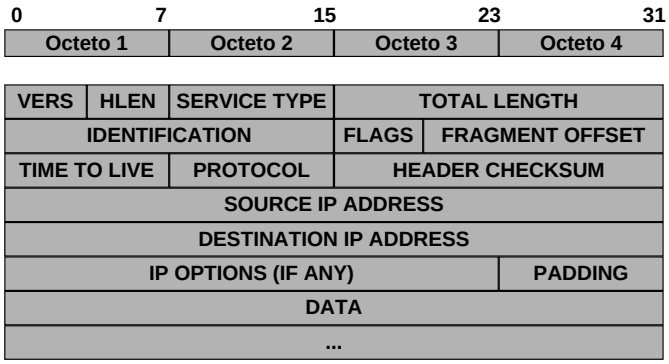
Como exemplos de rotas definidas estaticamente, pode-se citar:

- Uma rota default (ou roteador default) configurado manualmente nas estações (caso típico da maioria das estações-cliente em uma rede. P.ex., Janela de configuração básica de TCP/IP em Windows 3.1, Windows 95 e Windows NT
- Mais de uma rota default, com os roteadores configurados manualmente nas estações
- Rotas adicionais estáticas configuradas manualmente endereçando redes específicas. P.ex. Comando route add dos sistemas operacionais Windows 95 e Windows NT
- Roteadores descobertos através do protocolo ICMP Router Advertisement
- Rotas informadas através do protocolo ICMP Redirect

Pacote IP

O protocolo IP define a unidade básica de transmissão, que é o pacote IP. Neste pacote são colocadas as informações relevantes para o envio deste pacote até o destino.

O pacote IP possui o formato descrito abaixo:



Os campos mais importantes são descritos abaixo:

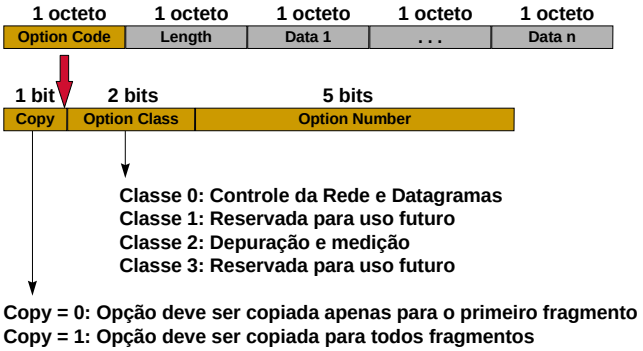
VERSION - Informa a versão do protocolo IP sendo carregado. Atualmente a versão de IP é 4

HEADER LENGTH - Informa o tamanho do header IP em grupos de 4 bytes

TYPE OF SERVICE - Informa como o pacote deve ser tratado, de acordo com sua prioridade e o tipo de serviço desejado como Baixo Retardo, Alta Capacidade de Banda ou Alta Confiablilidade. Normalmente este campo não é utilizado na Internet

IDENTIFICATION - Identifica o pacote IP unicamente entre os outros transmitidos pela máquina. Este campo é usado para identificar o pacote IP no caso de haver fragmentação em múltiplos datagramas
FLAGS (3 bits) - um bit (MF - More Fragments) identifica se este datagrama é o último fragmento de um pacote IP ou se existem mais. Outro bit (DNF - Do Not Fragment) informa aos roteadores no caminho se a aplicação exige que os pacotes não sejam fragmentados.
FRAGMENT OFFSET - Informa o posicionamento do fragmento em relação ao pacote IP do qual faz parte.
TIME-TO-LIVE - Este valor é decrementado a cada 1 segundo que o pacote passa na rede e a cada roteador pelo quel ele passa. Serve para limitar a duração do pacote IP e evitar que um pacote seja roteador eternamente na Internet como resultado de um loop de roteamento.
PROTOCOL - Informa que protocolo de mais alto-nível está sendo carregado no campo de dados. O IP pode carregar mensagens UDP, TCP, ICMP, e várias outras.
HEADER CHECKSUM - Valor que ajuda a garantir a integridade do cabeçalho do pacote IP
SOURCE ADDRESS - Endereço IP da máquina origem do pacote IP
DESTINATION ADDRESS - Endereço IP da máquina destino do pacote IP
OPTIONS - Opções com informações adicionais para o protocolo IP. Consiste de um byte com a identificação da opção e uma quantidade de bytes variável com as informações específicas. Um pacote IP pode transportar várias opções simultaneamente.

Opções IP
O formato das opções IP é descrita no quadro abaixo:

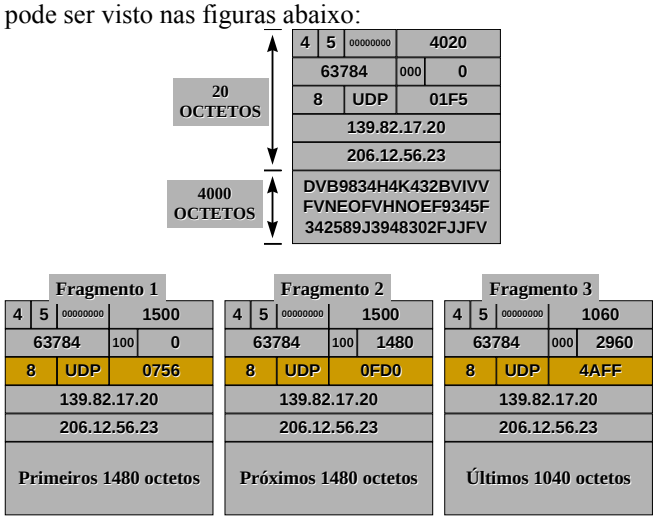


As opções IP que podem ser utilizadas são:

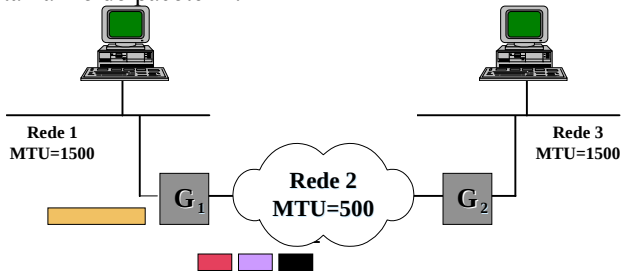
Classe	Código	Composição	Descrição
0	0	--	Fim da Lista de Opções
0	1	--	Nenhuma Operação
0	3	variável	LOOSE SOURCE ROUTING (Especifica a rota aproximada que um datagrama deve seguir)
0	7	variável	RECORD ROUTE (Escreve os endereços dos roteadores por onde o pacote passou)
0	9	variável	STRICT SOURCE ROUTING (Especifica a rota exata que um datagrama deve seguir)
2	4	variável	INTERNET TIMESTAMP (A cada roteador grava a hora da passagem para outra rede)

As opções IP são utilizadas basicamente como forma de verificação e monitoração de uma rede IP. As opções que especificam a rota até o destino não são utilizadas normalmente pois o IP é baseado na técnica de Next-Hop routing. Ainda assim, estes mecanismos são pouco utilizados como ferramenta de testes e verificação, sendo raros os programas que os implementam.

Fragmentação
Um pacote IP pode ter um tamanho de até 64 Kbytes. Entretanto o nível de rede geralmente tem um tamanho máximo menor que 64K. Por exemplo, uma rede Ethernet pode transmitir uma mensagem de até 1500 bytes. Este valor é chamado de MTU - Maximum Transmission Unit - para este tipo de rede. A camada IP deve então ser capaz de dividir um pacote IP maior que 1500 bytes em diversos fragmentos de até 1500 bytes cada um.
A fragmentação do pacote IP pode ocorrer na máquina origem ou em algum roteador que possua uma rede com MTU menor que o tamanho do pacote IP sendo roteado. Note que durante o percurso até o destino, um fragmento pode ser novamente fragmentado se o MTU da rede seguinte for ainda menor que o tamanho do fragmento. A remontagem do pacote só é realizada pela máquina destino, baseado nas informações de FRAGMENT OFFSET e bit MF. A perda de um fragmento inutiliza o datagrama inteiro.
O campo FRAGMENT OFFSET identifica a posição em Bytes do fragmento face ao pacote IP completo conforme pode ser visto nas figuras abaixo:



A figura abaixo mostra a fragmentação de um pacote quando este passa para uma rede com MTU menor que o tamanho do pacote IP.



Endereçamento em Subredes

A divisão de endereçamento tradicional da Internet em classes, causou sérios problemas de eficiência na distribuição de endereços. Cada rede na Internet, tenha ela 5, 200, 2000 ou 30 máquinas deveria ser compatível com uma das classes de endereços. Desta forma, uma rede com 10 estações receberia um endereço do tipo classe C, com capacidade de endereçar 256 estações. Isto significa um desperdício de 246 endereços. Da mesma forma, uma rede com 2000 estações receberia uma rede do tipo classe B, e desta forma causaria um desperdício de 62000 endereços.

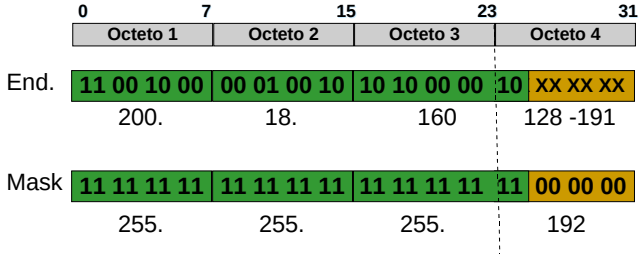
O número de redes interligando-se à Internet a partir de 1988 aumentou, causando o agravamento do problema de disponibilidade de endereços na Internet, especialmente o desperdício de endereços em classes C e B. Desta forma, buscou-se alternativas para aumentar o número de endereços de rede disponíveis sem afetar o funcionamento dos sistemas existentes. A melhor alternativa encontrada foi flexibilizar o conceito de classes - onde a divisão entre rede e host ocorre somente a cada 8 bits.

A solução encontrada foi utilizar a identificação de rede e host no endereçamento IP de forma variável, podendo utilizar qualquer quantidade de bits e não mais múltiplos de 8 bits conforme ocorria anteriormente. Um identificador adicional, a MÁSCARA, identifica em um endereço IP, que porção de bits é utilizada para identificar a rede e que porção de bits para host.

A máscara é formada por 4 bytes com uma sequência contínua de 1's, seguida de uma sequência de 0's. A porção de bits em 1 identifica quais bits são utilizados para identificar a rede no endereço e a porção de bits em 0, identifica que bits do endereço identificam a estação.

Obs. A máscara pode ser compreendida também como um número inteiro que diz a quantidade de bits um utilizados. Por exemplo uma máscara com valor 255.255.255.192, poderia ser representada como /26. Este tipo de notação é empregada em protocolos de roteamento mais recentes

Este mecanismo está representado na figura abaixo:

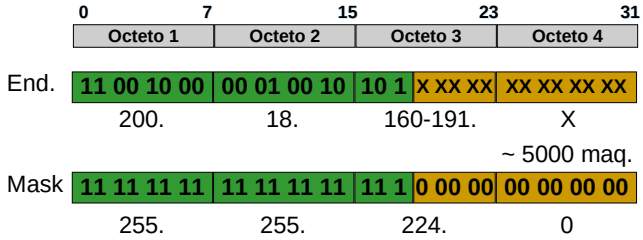


Neste endereço 200.18.160.X, a parte de rede possui 26 bits para identificar a rede e os 6 bits restantes para identificar os hosts. Desta forma, o endereço 200.18.160.0 da antiga classe C, fornecido a um conjunto de redes pode ser dividido em quatro redes com as identificações abaixo. Note que os 4 endereços de rede são independentes entre si. Elas podem ser empregadas em redes completamente separadas, e até mesmo serem utilizadas em instituições distintas.

200.18.160.[00XXXXXX]
200.18.160.[01XXXXXX]
200.18.160.[10XXXXXX] e
200.18.160.[11XXXXXX]

Em termos de identificação da rede, utiliza-se os mesmos critérios anteriores, ou seja, todos os bits de identificação da estação são 0. Quando os bits da estação são todos 1, isto identifica um broadcast naquela rede específica. Desta forma temos as seguintes identificações para endereço de rede:
200.18.160.0
200.18.160.64
200.18.160.128 e
200.18.160.192
Os endereços de broadcast nas redes são:
200.18.160.63
200.18.160.127
200.18.160.191 e
200.18.160.255
Os possíveis endereços de estação em cada rede são:
200.18.160.[1-62]
200.18.160.[65-126]
200.18.160.[129-190] e
200.18.160.[193-254]

O mesmo raciocínio de subrede pode ser usado para agrupar várias redes da antiga classe C em uma rede com capacidade de endereçamento de um maior número de hosts. A isto dá-se o nome de superrede. Hoje, já não há mais esta denominação pois não existe mais o conceito de classes. Um endereço da antiga classe A, como por exemplo 32.X.X.X pode ser dividido de qualquer forma por meio da máscara.



As máscaras das antigas classes A, B e C são um sub-conjunto das possibilidades do esquema utilizado atualmente, conforme mostrado abaixo:
Classe A: máscara equivalente = 255.0.0.0
Classe B: máscara equivalente = 255.255.0.0
Classe C: máscara equivalente = 255.255.255.0

1.7. Flexibilidade de Endereçamento

Uma conclusão que pode-se obter da análise acima é que uma identificação de uma rede, composta de um endereço de rede e uma máscara (p.ex. 200.18.171.64 e máscara 255.255.255.192) é, na verdade, um espaço de endereçamento, que pode ser usado da forma mais indicada. Por exemplo um espaço de endereçamento dado por

Rede = 32.10.20.128 com máscara 255.255.255.192

pode endereçar 64 endereços (62 endereços válidos) em uma rede só. Mas podemos subdividi-lo em subredes, de tal forma que poderemos ter:

- 1 rede de 64 endereços (usando o endereço e a máscara como estão)

- 2 redes de 32 endereços (aumentando em mais um bit a máscara)

Neste caso temos o endereço 32.10.20.128 dividido da seguinte forma:

Rede 1 = 32.10.20.128 com máscara 255.255.255.224 e

Rede 2 = 32.10.20.160 com máscara 255.255.255.224

Neste caso, cada rede formada pode ter até 30 endereços, pois deve-se sempre reservar os bits TODOS ZERO para o endereço de rede e os bits TODOS UM para o endereço de broadcast.

Desta forma, os endereços de máquina em cada rede são:

Rede 1: 32.10.20.[129-158] e

Rede 2: 32.10.20.[161-190]

Note que deve-se sempre respeitar o espaço de endereçamento original. Um dos erros mais comuns é utilizar parte do endereçamento vizinho, o que está errado pois pertence a outro espaço de endereçamento.

- 4 redes de 16 endereços (aumentando em dois bits a mascara original)

Neste caso temos o endereço 32.10.20.128 dividido da seguinte forma:

Rede 1 = 32.10.20.128 com máscara 255.255.255.240

Rede 2 = 32.10.20.144 com máscara 255.255.255.240

Rede 3 = 32.10.20.160 com máscara 255.255.255.240

Rede 4 = 32.10.20.176 com máscara 255.255.255.240

Neste caso, cada rede formada pode ter até 14 estações

Então os endereços de máquina em cada rede são:

Rede 1: 32.10.20.[129-142]

Rede 2: 32.10.20.[145-158]

Rede 3: 32.10.20.[161-174]

Rede 4: 32.10.20.[177-190]

Note que o espaço de endereçamento original sempre se manteve, variando de 128 a 191

- 8 redes de 8 endereços
- 16 redes de 4 endereços (onde 4 endereços são na verdade duas estações, devido aos endereços reservados de rede e broadcast)
- E só ! pois 32 redes de 2 estações não existe pois seria uma rede sem nenhuma estação pois os dois endereços disponíveis já seriam utilizados para rede e broadcast.

Entretanto, as formas acima ainda não são as únicas formas de divisão do espaço de endereçamento. Pode-se dividir em mais uma dezena de forma, utilizando-se divisões do espaço de endereçamento de forma não homogênea. Um exemplo claro pode ser dado por exemplo observando redes reais, onde a quantidade de estações pode variar bastante entre cada uma. Por exemplo, supondo que o espaço de endereçamento acima com capacidade de endereçar 64 estações deva ser utilizado em uma empresa com 50 estações. Estas 50 estações estão divididas em 3 redes, sendo uma com 30 estações e duas com 10 estações. Pode-se observar que nenhuma das formas de divisão acima são aceitáveis pois ou não comportam o número de redes necessárias (divisão em duas) ou não comportam o número de estações (divisão em 4).

A solução é realizar uma divisão do espaço de endereçamento de forma não homogênea. Isto é realizado de forma simples, utilizando metade do espaço original para a rede de 30 estações e dividindo o espaço restante em duas redes de 16 endereços.

De forma resumida, a divisão é da seguinte forma:

O espaço original; é dividido em dois, onde temos duas redes de 32 endereços:

Rede 1 = 32.10.20.128 com máscara 255.255.255.224

Rede 2 = 32.10.20.160 com máscara 255.255.255.224

Utiliza-se a rede 1 que possui os endereços de estação 32.10.20[129-158] para a rede com 30 estações. A rede 2 é na verdade um outro espaço de endereçamento (!) dado por 32.10.20.160 com máscara 255.255.255.224. Pode-se então dividir este espaço de endereçamento em duas rede, bastando aumentar um bit na máscara de rede:

Rede 2 = 32.10.20.160 com máscara 255.255.255.240

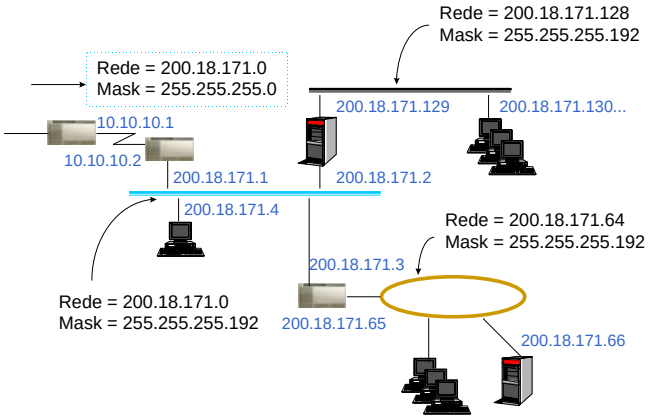
Rede 3 = 32.10.20.176 com máscara 255.255.255.240

Então, o resultado final são três redes, onde a rede 2 possui os endereços de rede 32.10.20.[161-174] para estações e a rede 3 possui os endereços 32.10.20.[177-190] para as estações.

A figura abaixo mostra um exemplo de redes de uma empresa que ao se ligar à Internet, recebeu o espaço de endereçamento 200.18.171.0 com máscara 255.255.255.0 para ser utilizado em suas 3 redes internas. As rede possuem cada uma 50 estações, de modo que a divisão mais adequada é dividir o espaço em 4 redes de 64 endereços.

Neste caso o espaço de endereçamento 200.18.171.0 com máscara 255.255.255.0 foi dividido em três subredes, cada uma com capacidade de endereçar até 62 estações (64 endereços retirando o [000000] e o [111111]).

Note neste exemplo, que para a Internet, as três redes são vistas como uma só pois as rotas na Internet sempre se referem à rede 200.18.171.0 com máscara 255.255.255.0. Por isto os termos rede e espaço de endereçamento são utilizados de forma indistinta.



1.8. Roteamento com Sub-rede

Com a utilização de sub-rede, a tabela de rotas possui um campo adicional que é a mascara de rede, já que a identificação de uma rede possui uma máscara.

No caso do exemplo anterior, um roteador qualquer na Internet que conecte este conjunto de redes à Internet possui apenas uma rota para a rede 200.18.171.0, com máscara 255.255.255.0, endereçada para o roteador 10.0.0.1. Isto mostra que a informação roteamento das diversas sub-redes pode ser agregada em uma única linha na tabela de rotas.

Por exemplo apesar de possuir centenas de redes, os roteadores na Internet possuem uma única linha para a PUC, sendo a rede destino 139.82.0.0 e a máscara 255.255.0.0. somente dentro da PUC, os roteadores internos devem saber distinguir as diversas sub-redes formadas.

No exemplo anterior, o roteador interno da empresa não pode ter uma rota genérica para a rede 200.18.171.0, mas precisa saber endereçar as diversas sub-redes. Isto se dá pela utilização de rotas associadas a máscara. A tabela abaixo mostra a tabela de rotas deste roteador:

Rede Destino	Máscara	Roteador (Gateway)	Hops
200.18.171.0	255.255.255.192	200.18.171.1 (eth0)	0
10.0.0.0	255.0.0.0	10.0.0.1 (serial1)	0
200.18.171.64	255.255.255.192	200.18.171.3	1
200.18.171.128	255.255.255.192	200.18.171.2	1
default	0.0.0.0	10.0.0.2	--

A tabela de rotas do roteador inferior é dada pela tabela abaixo:

Rede Destino	Máscara	Roteador (Gateway)	Hops
200.18.171.0	255.255.255.192	200.18.171.3 (eth0)	0
200.18.171.64	255.255.255.192	200.18.171.65 (eth1)	0
200.18.171.128	255.255.255.192	200.18.171.2	1
default	0.0.0.0	200.18.171.1	--

A máscara de rede faz parte de toda tabela de rotas.

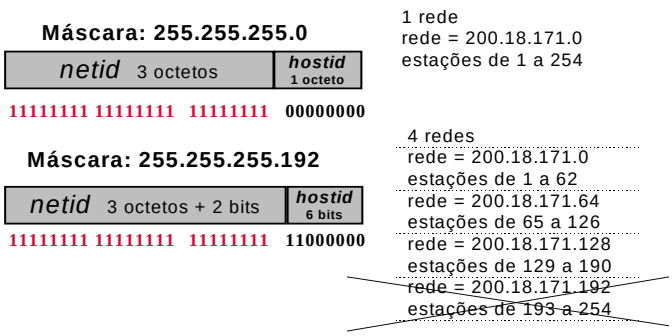
O algoritmo de Recepção de pacote IP e roteamento com a introdução da máscara de sub-rede fica alterado conforme abaixo:

1. Datagrama recebido da camada intra-rede, defragmentado e testado
2. Caso:
   2.1 Endereço Destino = Endereço do Host, ou E.D. = outras interfaces do Host, ou E.D. = Broadcast
      2.1.1 Passa datagrama para níveis superiores -> FIM
   2.2 Caso:
      2.2.1 Máquina que recebeu não é roteador
         2.2.1.1 Descarta datagrama -> FIM
      2.2.2 Máquina é roteador (possui mais de uma interface IP)
         2.2.2.1 Caso:
            2.2.2.1.1 Endereço de rede IP destino = Alguma das Redes IP com interface direta
               2.2.2.1.1.1 Descobre o endereço físico do destino (ARP)
               2.2.2.1.1.2 Transmite datagrama pela interface respectiva -> FIM
            2.2.2.1.2 Faz um AND lógico bit-a-bit do endereço IP com as máscaras de cada rede da tabela de rotas e compara com o endereço de rede da rota respectiva
            2.2.2.1.3 Se algum conferir, descobriu uma rota
               2.2.2.1.3.1 Verifica na tabela de rotas o endereço IP do roteador destino desta rota.
               2.2.2.1.3.2 Descobre o endereço físico do gateway (ARP)
               2.2.2.1.3.3 Transmite o datagrama para o gateway -> FIM
3. Fim

Sub-Redes não utilizáveis:

Devido a motivos históricos do desenvolvimento de TCP/IP, a divisão em sub-redes tem algumas restrições quanto a utilização de algumas sub-redes. Basicamente, não se pode utilizar o endereçamento que contêm todos os bits UM da porção da sub-rede. As implementações mais novas permitem que este endereçamento seja utilizado.

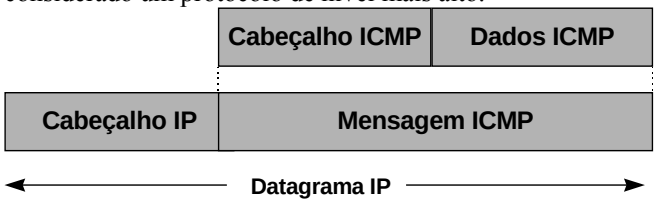
A figura abaixo ilustra esta restrição na utilização da sub-rede com os dois bits 11, para o caso da máscara 255.255.255.192. No caso da utilização da máscara 255.255.255.224, não se deve utilizar a sub-rede com bits 111.



Protocolo ICMP

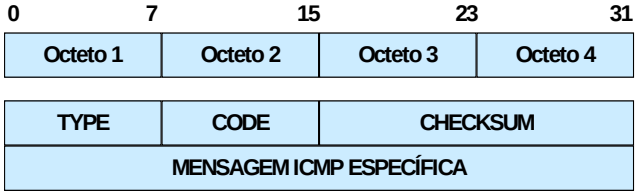
O protocolo ICMP é um protocolo auxiliar ao IP, que carrega informações de controle e diagnóstico, informando falhas como TTL do pacote IP expirou, erros de fragmentação, roteadores intermediários congestionados e outros.

Uma mensagem ICMP é encapsulada no protocolo IP, conforme ilustrado na figura abaixo. Apesar de encapsulado dentro do pacote IP, o protocolo ICMP não é considerado um protocolo de nível mais alto.



A mensagem ICMP é sempre destinada ao host origem da mensagem, não existindo nenhum mecanismo para informar erros aos roteadores no caminho ou ao host destino.

As mensagens ICMP possuem um identificar principal de tipo (TYPE) e um identificador de sub-tipo (CODE), conforme pode ser visto no formato de mensagem ilustrado abaixo:



Os tipos de mensagem ICMP são listados na tabela abaixo:

Tipo	Mensagem ICMP	Categoria
0	Echo Reply	Controle
3	Destination Unreachable	Erro
4	Source Quench	Controle
5	Redirect	Controle
8	Echo Request	Controle
9	Router Advertisement (RFC 1256)	Controle
10	Router Solicitation (RFC 1256)	Controle
11	Time Exceeded for a Datagram	Erro
12	Parameter Problem on a Datagram	Erro
13	Timestamp Request	Controle
14	Timestamp Reply	Controle
15	Information Request (obsoleto)	Controle
16	Information Reply (obsoleto)	Controle
17	Address Mark Request	Controle
18	Address Mark Reply	Controle

ARP (ADDRESS RESOLUTION PROTOCOL) – protocolo que converte Endereço IP(lógico) em endereço MAC(físico).

RARP (REVERSE ADDRESS RESOLUTION PROTOCOL) – protocolo que converte Endereço MAC (físico) em endereço IP (lógico).

Camada de Interface de Rede.

A camada deInterface de rede é responsável pelo envio de datagramas construídos pela camada Inter-Rede. Esta camada realiza também o mapeamento entre um endereço de identificação de nível Inter-rede para um endereço físico ou lógico do nível de Interface de Rede. A camada Inter-Rede é independente do nível de Interface.

Alguns protocolos existentes nesta camada são:

- Protocolos com estrutura de rede própria (X.25, Frame-Relay, ATM)
- Protocolos de Enlace OSI (PPP, Ethernet, Token-Ring, FDDI, HDLC, SLIP, …)
- Protocolos de Nível Físico (V.24, X.21)
- Protocolos de barramento de alta-velocidade (SCSI, HIPPI, …)
- Protocolos de mapeamento de endereços (ARP - Address Resolution Protocol) - Este protocolo pode ser considerado também como parte da camada Inter-Rede.

Os protocolos deste nível possuem um esquema de identificação das máquinas interligadas por este protocolo. Por exemplo, cada máquina situada em uma rede Ethernet, Token-Ring ou FDDI possui um identificador único chamado endereço MAC ou endereço físico que permite distinguir uma máquina de outra, possibilitando o envio de

mensagens específicas para cada uma delas. Tais rede são chamadas redes locais de computadores.
Da mesma forma, estações em redes X.25, Frame-Relay ou ATM também possuem endereços que as distinguem uma das outras.
As redes ponto-a-ponto, formadas pela interligação entre duas máquinas não possuem, geralmente, um endereçamento de nível de rede (modelo TCP/IP), uma vez que não há necessidade de identificar várias estações.

PPP (PROTOCOL POINT-TO-POINT) – é um protocolo criado na conexão entre dois pontos, tipicamente dois modems. Interessante notar que, apesar de ter sido criado para transportar datagramas IP, esse protocolo também pode ser utilizado por outros protocolos, como o IPX/SPX.

ETHERNET

A arquitetura Ethernet é a mais usada em redes locais. O Ethernet é um padrão que define como os dados serão transmitidos fisicamente através dos cabos da rede. Dessa forma, essa arquitetura – assim como as arquiteturas Token Ring e FDDI – opera nas camadas 1 e 2 do modelo OSI.

O papel do Ethernet é, portanto, pegar os dados entregues pelos protocolos de alto nível – TCP/IP, IPX/SPX, NetBEUI, etc e inseri-los dentro de quadros que serão enviados através da rede. O Ethernet define também como fisicamente esses dados serão transmitidos (o formato do sinal, por exemplo).

As camadas do modelo OSI podem ser substituídas pelas camadas do protocolo que estiver sendo usado. Por exemplo, em uma rede local baseada no protocolo TCP/IP usando a arquitetura Ethernet, onde a camada de interface com a rede do protocolo TCP/IP é o padrão Ethernet.

As três camadas da arquitetura Ethernet possuem as seguintes funções:

- **Controle do Link Lógico (LCC, IEEE 802.2) –** Inclui informações do protocolo de alto nível que entregou o pacote de dados a ser transmitido. Com isso, a maquina receptora tem como saber para qual protocolo de alto nível ela deve entregar os dados de um quadro que ela acabou de receber.
- **Controle de Acesso ao Meio (MAC, IEEE 802.3) –** Monta o quadro de dados a ser transmitido pela camada física, incluindo cabeçalhos próximos dessa camada aos dados recebidos da camada de Controle do Link Lógico.
- **Física –** Transmite os quadros entregues pela camada de Controle de Acesso ao Meio usando o método CSMA/CD (Carrier Sense Multiple Access with Collision Detection), que estudaremos a seguir. Define como os dados são transmitidos através do cabeamento da rede e também o formato dos conectores usados na placa de rede.

A camada FÍSICA.
O próximo tópico a ser abordado é o funcionamento da camada física da arquitetura Ethernet: o padrão CSMA/CD, a codificação dos dados e a placa de rede.

OSI	ETHERNET
Link de Dados	Controle do link lógico (LCC) – IEEE 802.2
	Controle de Acesso ao Meio (MAC) – IEEE 802.3
Física	Física

CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Em redes Ethernet, todos os micros compartilham o mesmo cabo, independentemente da topologia utilizada. Mesmo em redes Ethernet montadas com um topologia em estrela usando um periférico chamado HUB isso ocorre. Isso significa que, quando o cabo esta sendo utilizado, nenhuma outra máquina poderá usa-lo ao mesmo tempo.

Por exemplo, se em uma rede uma máquina B está transmitindo para A nenhuma outra máquina poderá utilizar o cabo; elas terão de esperar o cabo ficar livre.

Assim, o primeiro passo na transmissão de dados em uma rede Ethernet é verificar se o cabo está livre. Isso é feito pela placa de rede e daí o nome *Carrier Sense* (detecção de portadora). Se o cabo estiver livre, a placa de rede inicia sua transmissão. Caso ele esteja ocupado, a placa espera até que ele fique livre (não exista mais o sinal de portadora no cabo). A transmissão só será iniciada caso o cabo esteja livre.

Entretanto, o protocolo CSMA/CD não gera nenhum tipo de prioridade (daí o nome *Multiple Access*, acesso múltiplo). Com isso, pode ocorrer de duas ou mais placas de redes perceberem que o cabo esta livre e tentarem transmitir dados ao mesmo tempo. Quando isso ocorre, há uma colisão e nenhuma das placas consegue transmitir dados.

Quando ocorre uma colisão, todas as placas de rede param de transmitir, esperam um período de tempo aleatório, e tentam a retransmissão. Como cada placa de rede envolvida na colisão provavelmente gerará um valor aleatório diferente, possivelmente não ocorrerá novamente outra colisão, pois uma das placas começará a sua transmissão antes das demais. E as demais verificarão que o cabo está ocupado e na tentarão transmitir.

Só que existe a possibilidade de haver sempre novas colisões, caso outras placas de rede que não estavam envolvidas nessa primeira colisão tentem transmitir dados justamente no mesmo momento em que terminou o tempo de espera de uma das placas de rede envolvidas na colisão.

Como sempre que há colisão é necessário gerar um período de espera, o desempenho de redes Ehternet está intimamente ligado ao número de máquinas existentes na rede. Quanto mais máquinas, maior a probabilidade de ocorrerem colisões e, com isso, o desempenho da rede cai, já que haverá períodos de espera.

Outros protocolos utilizados em redes e na internet.

O protocolo OSI – O modelo de referência OSI (*Open System Interconnection)* é conhecido como modelo de padronização de tecnologias de redes de computadores. O modelo OSI teve como objetivo estabelecer uma regra e direcionamento no desenvolvimento de modelos de arquiteturas de redes. O modelo OSI nasceu da necessidade de criar um protocolo que conseguisse se

comunicar entre redes diferentes. O protocolo OSI é dividido em sete camadas:

7	Aplicação
6	Apresentação
5	Sessão
4	Transporte
3	Rede
2	Enlace
1	Física

Aplicação – trabalha com a interface entre o protocolo e o aplicativo.

Apresentação – faz a tradução das informações colocando-as em um formato que possa ser entendido pelas outras camadas. A camada de apresentação também é usada para *compressão de dados* (trabalha no sentido de diminuir o tamanho do pacote) e *criptografia* (criptografa os pacotes que só poderão ser descriptografados na camada 6 do receptor.

Sessão – marca os dados para estabelecer que computadores diferentes tenham uma sessão de comunicação. Se ocorrer uma falha na comunicação o processo poderá ser reiniciado do mesmo ponto.

Transporte – faz a ligação entre as camadas do nível de aplicação (5, 6 e 7) com as camadas do nível físico (1, 2 e 3). A camada de transporte pega os dados da camada de sessão e faz a divisão em pacotes. Na camada física, os pacotes da camada de transporte serão transformados em quadros.

Rede – recebe os pacotes da camada de transporte ou quadros da camada link de dados e faz o endereçamento dos dados (pacotes) convertendo o endereço lógico em endereço físico para que os pacotes possam chegar corretamente ao destino. Serve também para indicar a rota que o pacote vai seguir da origem ao destino.

Link de Dados (Enlace) – recebe os dados da camada de rede e converte em quadros que serão enviados colocando o endereço físico (placa de rede destino), dados de controle e CRC. CRC (*Cyclical Redundancy Check*) ou *Checksum* ocorre quando a informação chega à camada Link de Dados do receptor então essa camada emite uma confirmação de chegada ACK (Acknowledge), ou seja, realiza o CRC. Se a confirmação não chegar o transmissor reenvia o quadro.

Física – recebe os dados e converte em sinais que deverão ser enviados pela rede. A camada física especifica a maneira com que os 0s e 1s dos quadros serão enviados para a rede (ou recebidos da rede, no caso da recepçao de dados).

NetBEUI/NetBIOS

O NetBEUI, NetBIOS Enchanced User Interface, é um protocolo proprietário da Microsoft, que acompanha todos os seus sistemas operacionais e produtos de redes, como o Windows 9x/ME, Windows NT/2000. este protocolo é utilizado como base para o NetBIOS (Network Basic Input/Output System) para compartilhamento de arquivos e impressoras.

O NetBEUI é protocolo pequeno e rápido. Porém possui duas grandes desvantagens:

→ comunicação por broadicast; o que pode inviabilizar seu uso se a quantidade de hosts for muito grande.

→ é um protocolo não roteável. Isso significa que não pode ser usado em redes que possuem outras redes interconectadas, isto é, que utilizem roteadores para se comunicar.

SPX/IPX

O Sequenced Packet Exchange/Internet Packet Exchange é o protocolo utilizado pela rede Novell. Implementa as camadas 3 e 4 do modelo de referência OSI, e utiliza, como protocolo de camada 2, exclusivamente o Ethernet (é um padrão que define como os dados serão transmitidos fisicamente através dos cabos da rede). Por muitos anos, Netware e Ethernet foram considerados sinônimos. Possuem diversas semelhanças com o TCP/IP. Já foram os protocolos mais populares, mas sendo o TCP/IP a base da Internet, acabaram caindo em desuso.

→ **IPX –** O IPX seria o equivalente ao protocolo de redes. É uma implementação muito volumosa e cheia de recursos. Tem algumas características vantajosas como a detecção de endereços MAC e atribuição automática de endereço IPX, ao contrário de outros protocolos como o IP, que fazem com o usuário tenha de atribuir manualmente um endereço para cada interface ou configurar um serviço externo que automatize a tarefa.

→ **SPX –** Da mesma forma que IPX, o SPX tem correspondência com o protocolo OSI de transporte. Uma das características mais importantes dessa implementação é que o SPX tem de receber a confirmação dos pacotes enviados antes de poder enviar outro, o que traz prejuízos para o desempenho da rede.

APPLE TALK

O *Appletalk*, como o próprio nome sugere, é o protocolo proprietário utilizado nas redes de computadores Apple. É composto por protocolos de transporte e entrega, o ATP (Apple Talk Transport Protocol) é o DDP (Datagram Delivery Protocol), equivalentes às camadas 4 3 do modelo OSI.

PROTOCOLO X.25

O protocolo X.25 é um protocolo de acesso a WANS que define regras de comunicação entre equipamentos DTE (roteadores, terminais) e uma rede (DCE) de pacotes que tanto pode ser pública quanto privada. O protocolo define regras para o perfeito estabelecimento , transmissão, recepção de dados, controle de fluxo e desconexão entre equipamentos. O X.25 surgiu com o objetivo de evitar que redes públicas geograficamente distribuídas desenvolvessem diferentes interfaces de acesso.

FRAME RELAY

O frame relay é um protocolo baseado em redes comutadas, assim como o X.25. A grande diferença é que o Frame Relay, ao contrário do X.25, é um protocolo orientado à conexão, sem controle de erros e nenhum controle de fluxo. Portanto, em redes usando o Frame Relay, a entrega dos dados não é garantida.

A vantagem do Frame Relay em relação ao X.25 é a velocidade. Por não possuir nenhum mecanismo para verificar se o datagrama chegou ou não ao destino, este protocolo consegue ser mais rápido do que o X.25, já que no X.25 o receptor precisa enviar uma informação de confirmação (acknowledge) ao transmissor a cada pacote recebido.

PROTOCOLO DHCP

DHCP é um acrônimo para Protocolo de Configuração Dinâmica de Computador (Dinamic Host Configuration Protocol). É um protocolo cliente/servidor, que possibilita computadores clientes receberem configurações TCP/IP dinamicamente. Esta funcionalidade tem muita importância em grandes redes, pois o controle das configurações TCP/IP é feito de forma centralizada, tornando esta configuração praticamente transparente para o administrador.

PROTOCOLO ATM

ATM (Asynchronous Transfer Mode) é uma tecnologia baseada na transmissão de pequenas unidades de informação de tamanho fixo denominadas "células" que são transmitidas através de circuitos virtuais. Redes ATM funcionam com o mesmo princípio do X.25: são redes comutadas orientadas à conexão. A grande diferença são as altas taxas de transferência obtidas pelo ATM, que variam entre 25 e 622 Mbps.

Tecnologia ATM

Suporte do tráfico *broadcast*

A evolução das aplicações que requerem transporte digital mostra, desde faz tempo, uma clara mudança de rumo de meios ponto a ponto a meios pontos a multipontos. Aplicações como videoconferências, tráfico LAN, broadcasting de vídeo, etc. requerem de suporte *broadcast* na capa de transporte.

Antes da ATM, as tecnologias de transporte digital, baseavam-se na multiplexação sobre canais ponto a ponto e, portanto, não podiam enfrentar-se a este novo requerimento de serviço.

ATM, ainda que seja uma tecnologia orientada à conexão contempla o uso de circuitos ponto-multiponto que permitem oferecer funções de broadcasting de informação. Os dados se replicam no interior da rede ali onde se divide o circuito ponto-multiponto. Esta aproximação minimiza o largo de banda associado ao tráfico *broadcast* e permite a extensão e crescimento destes serviços até níveis muito elevados.

Canais comutados

Outro requerimento que se lhe pediu a ATM foi que dispusesse de mecanismos para o estabelecimento de circuitos comutados sob demanda do DTE. Estas funcionalidades que, até a data, só se exigiam às redes de banda estreita (RTC, RDSI, X.25, Frame Relay,…) fazem-se, cada vez mais, necessárias na capa de banda larga (Cabo - TV, Videoconferência,…) ATM define um protocolo de sinalização entre o DTE e a rede, chamado UNI, que permite a este segundo, a negociação de canais comutados sob demanda. O protocolo, baseado no Q.931 de RDSI, permite ao DTE a criação de um canal (ponto a ponto ou multiponto) com uma determinada qualidade de serviço (largo de banda, retardo,…).

Outro protocolo (NNI) encarrega-se da propagação da petição de telefonema dentro do interior da rede para o destino para sua aceitação. O NNI é um protocolo não orientado à conexão que permite a propagação de telefonemas por múltiplos caminhos alternativos.

No momento de definição de ATM se optou por um sistema de numeração de 20 bytes (baseado na numeração atual da rede telefônica básica) para os pontos terminais.

Escalabilidade

Um dos principais problemas com os que se encontram os administradores das redes de transporte é como atuar frente aos contínuos e cada vez mais freqüentes mudanças nos requerimentos tanto de cobertura como da largura de banda.

ATM se desenhou como uma rede "inteligente". O objetivo era que os nodos que compunham a rede fossem capazes de descobrir a topologia (nodos e enlaces) que lhes rodeava e criar-se uma imagem própria de como estava formada a rede. Ademais, este procedimento devia ser dinâmico para que a inserção de novos nodos ou enlaces na rede fossem detectados e assimilados automaticamente pelos outros nodos.

Esta filosofia de rede, que é muito comum nas redes de banda estreita (redes de routers,

Frame Relay, ...), implanta-se na banda larga com a tecnologia ATM.

Os administradores da rede de transporte ATM podem decidir livremente a mudança da largura de banda de um enlace ou a criação de um novo (por exemplo, para dispor de caminhos alternativos) sem ter que, por isso, reconfigurar de novo a rede. Todos os nodos afetados pela modificação topológica atuarão imediatamente como resposta à mudança (por exemplo, usando o novo enlace para balancear tráfico).

Os problemas de cobertura também não significam nenhum problema. Um nodo que se insere na rede descobre, e é descoberto por, o resto de nodos sem nenhuma intervenção por parte do administrador.

Tecnologia universal

Um balanço geral dos pontos anteriores permite ver como a tecnologia de transporte ATM incorpora e melhoram muitas das técnicas utilizadas unicamente, até então, nas redes de banda estreita. Isto quer dizer que ATM é também uma tecnologia válida para este tipo de redes.

ATM se define como uma tecnologia universal válida tanto como transporte digital de banda larga, como para backbone de alta velocidade em redes LAN ou integração de serviços em redes corporativas sobre enlaces de baixa

velocidade. ATM é uma solução global extremo a extremo; é tanto uma tecnologia de infra-estrutura como de aplicações.

Pontos firmes da tecnologia ATM
ATM se baseia num conjunto de novidades tecnológicas que fazem possível que cumpra os requerimentos a ela exigidos.

Padronização
Conquanto suas origens se remontam aos anos 60, é a partir de 1988 quando o CCITT ratifica a ATM como a tecnologia para o desenvolvimento das redes de banda larga (BRDSI), aparecendo os primeiros padrões em 1990.
Desde então até nossos dias ATM tem estado submetida a um rigoroso processo de padronização; destinado não somente a uma simples interoperabilidade a nível físico (velocidades SONET e SDH…), senão a garantir a criação de redes multifabricantes a nível de serviço, padronizando aspectos como Sinalização (UNI, NNI), Controle de Congestão, Integração LAN, etc.
Esta característica garante a criação de redes multifabricantes, que garantem o investimento e permitem um forte desenvolvimento do mercado, com a conseguinte redução de custos.

Multiplexação baseada em campos
Para que se possa gerar corretamente a largura de banda sobre um enlace, é necessário que as diferentes fontes que o utilizam apresentem seus dados em unidades mínimas de informação.
Para ATM se decidiu uma unidade mínima de 53 bytes fixos de tamanho. O uso de um tamanho fixo permite desenvolver módulos *hardwares* muito especializados que comutem estas celas às velocidades exigidas na banda larga (atuais e futuras). A longitude da unidade deve ser pequena para que se possa multiplexar rapidamente sobre um mesmo enlace, campos de diferentes fontes e assim garantir qualidade de serviço aos tráficos sensíveis (voz, vídeo,...)

Orientado à conexão
Como ATM é uma tecnologia orientada à conexão permitirá, entre outras coisas, conseguir uma unidade mínima de informação de tamanho pequeno. Como foi dito anteriormente, as previsões de crescimento para ATM nos obrigavam ao uso de um sistema de numeração de terminais de 20 bytes. As tecnologias não orientadas à conexão requerem que cada unidade de informação contenha em seu interior as direções tanto de origem como de destino. Obviamente, não se podiam dedicar 40 bytes de dados para esse objetivo (a sobrecarrega por quadro seria inaceitável).
Os únicos dados de direcionamento que se inclui no quadro é a identificação do canal virtual que supõe, unicamente, 5 bytes de dados (48 bytes úteis para a transmissão de informação).

Qualidade de Serviço (QoS)
Definem-se quatro categorias de tráfico básicas: CBR (*Constant Bit Rate*), VBR (*Variável Bit Rate*), UBR (*Undefined Bit Rate*) e AVR (*Available Bit Rate*) No momento da criação, o DTE caracteriza o tráfico que vai enviar pelo circuito mediante quatro parâmetros categóricos (PCR, SCR, CDVT e MBS). A rede propaga essa petição internamente até seu destino e valida se o requerimento exigido vão poder cumprir. Em caso afirmativo, a rede aceita o circuito e, a partir desse momento, garante que o tráfico seja tratado conforme as condições negociadas no estabelecimento.
Os comutadores ATM executam um algoritmo chamado *dual leaky buckets* que garante, quadro por quadro, que seja oferecida a qualidade de serviço requerido. É permitido que o DTE envie os dados por um circuito à velocidade maior da negociada. Nesse caso o comutador ATM pode proceder ao descarte dos quadros correspondentes em caso de saturação em algum ponto da rede.

Rede inteligente
Uma rede de transporte ATM é uma rede inteligente na qual cada nodo que a compõe é um elemento independente. Como se comentou anteriormente, os comutadores que formam a rede ATM descobrem individualmente a topologia de rede de seu meio mediante um protocolo de diálogo entre nodos.
Este tipo de aproximação, inovador nas redes de banda larga, abre as portas a um novo mundo de funcionalidades (enlaces de diferente velocidade, topologia flexível, balanço de tráfico, Escalabilidade,…) e é, sem lugar a dúvidas, a pedra angular da tecnologia ATM.

Topologia das redes ATM
Com tecnologia ATM se consegue criar uma rede de transporte de banda larga de topologia variável, isto é, em função das necessidades e enlaces disponíveis, o administrador da rede pode optar por uma topologia em estrela, malha, árvore, etc. com uma configuração livre de enlaces (E1, E3, OC-3 , …)

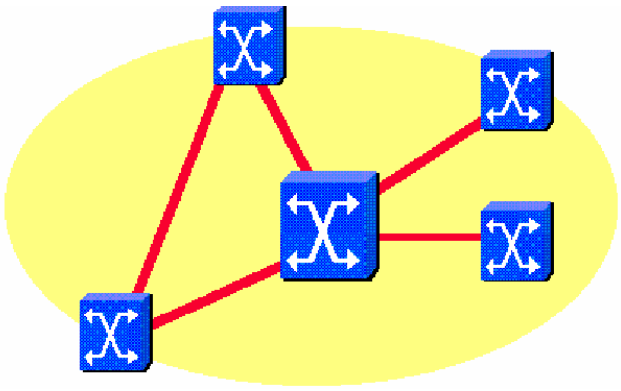


Figura – Topologia rede ATM

A grande vantagem é a indiscutível capacidade de adaptação às necessidades que ATM pode oferecer. Uma empresa pode começar a desenvolver sua rede de transporte de banda larga em base a umas premissas de largo de banda e cobertura obtidas a raiz de um estudo de necessidades. A evolução das aplicações pode conduzir a que uma dessas premissas fique obsoleta e que se precise uma redefinição do desenho. Neste caso, o administrador dispõe de total liberdade para mudar enlaces ou adicionar nodos onde seja necessário.

Modificação de enlaces

Suponhamos, por exemplo, o caso de uma dependência que antecede ao resto da rede de transporte ATM mediante um enlace E1 a 2Mbps. Por um crescimento inesperado no nome de trabalhadores em tal dependência, as necessidades de largura de banda ultrapassam o umbral dos 2Mbps que, no momento do desenho da rede considerou-se suficiente.

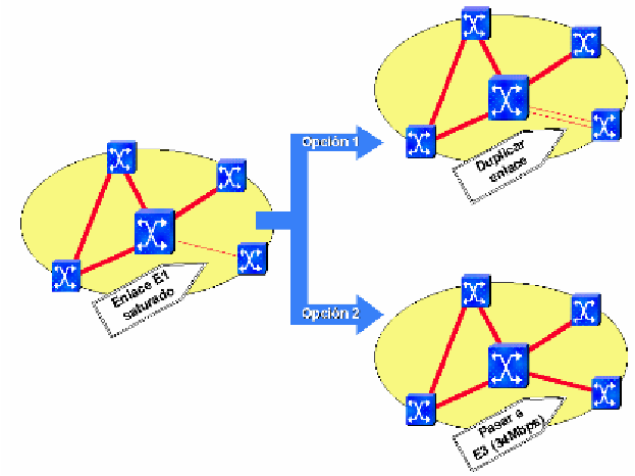


***Figura** - Liberdade de atuação frente a mudanças de enlace*

Ante esta situação, o administrador da rede pode optar por duas soluções. Uma delas consiste em contratar um segundo enlace E1 para o acesso da dependência (um agregado de 4Mbps) ou mudar o enlace principal ao outro nível na hierarquia (E3 a 34Mbps)

Qualquer das duas atuações será detectada instantaneamente pelos comutadores ATM afetados sem necessidade de reconfigurar a rede.

Ampliações sucessivas

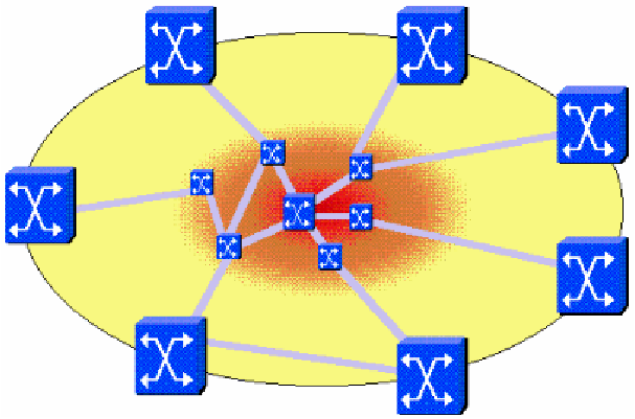


***Figura** - Crescimento ordenado em capas*

Outro problema muito freqüente com o que se encontram os administradores das redes de transporte é como adaptar-se às mudanças relativas a requerimentos de cobertura geográfica. Estas mudanças, que muitas vezes são devidos a mudanças estratégicas das empresas e, portanto imprevisíveis, estavam associados a graves problemas tecnológicos e econômicos antes da aparição da tecnologia ATM.

Como explicamos anteriormente, os novos nodos inseridos, são descobertos automaticamente pelo resto de comutadores que formam a rede ATM. O procedimento associado a adicionar uma nova dependência à rede de transporte ATM é tão singelo como eleger o tipo de enlace (E1, E3,…) e instalar o novo comutador. A rede responderá automaticamente a esta ampliação sem nenhuma necessidade de reconfigurar nada.

PNNI

Nos dois pontos anteriores explicamos que os comutadores que compõem uma rede ATM são capazes de detectar, dinamicamente, as mudanças de topologia que ocorrem a seu arredor. A base de todo este comportamento é a existência de um protocolo interno entre nodos: o PNNI

Um comutador ATM tenta, continuamente, estabelecer relações PNNI com outros comutadores por cada um de seus portos. Logo então, estabelece-se uma destas relações (por exemplo, entre dois comutadores adjacentes), procede-se a um intercâmbio de informação topológica entre eles. Desta maneira, cada comutador pode ter uma idéia de como esta desenhada a rede.

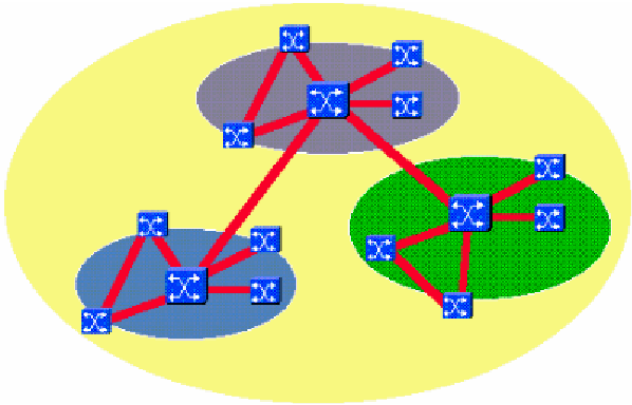


***Figura** - PNNI permite organizar as redes em áreas*

Frente a uma mudança topológica (inserção de um novo nodo, falha de um enlace existente) os nodos afetados notificam o evento através de suas relações PNNI ao resto de comutadores na rede. Este procedimento está baseado no algoritmo SPF (*Shortest Path First*).

Para permitir que este tipo de protocolo não represente um problema à Escalabilidade da rede, o PNNI usa uma aproximação hierárquica. A rede pode ser dividida em áreas dentro das quais se executa uma cópia independente do algoritmo. Cada área, a sua vez, pode estar composta por um número indeterminado de subáreas e assim indefinidamente. As redes baseadas em tecnologia ATM com PNNI podem crescer até mais de 2500 comutadores.

Transporte de serviços tradicionais

No campo das aplicações, uma rede de transporte digital ATM oferece um conjunto novo de funcionalidades disponíveis sem, por isso deixar de oferecer as funções tradicionais.

Imitação de circuito

Mediante a imitação de circuito, uma rede ATM pode se comportar exatamente igual a uma rede de transporte baseada em tecnologia SDH.

A técnica de imitação de circuito consiste na criação de um canal permanente sobre a rede ATM entre um ponto

origem e outro de destino a uma velocidade determinada. Este canal permanente se cria com características de velocidade de bit constante (CBR). Nos pontos extremos da rede ATM se dispõem interfaces elétricas adequadas à velocidade requerida (E1, V.35, V.11,…) e as equipes terminais a eles conectados dialogam transparentemente através da rede ATM.

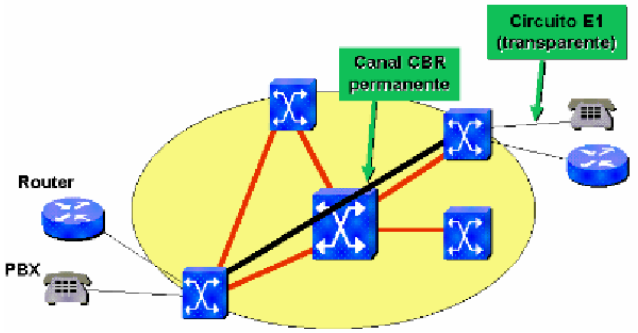


Figura *- Imitação de circuito*

Os dados que enviam os DTE nos extremos da imitação de circuito, são transformados em quadros e transmitidos através do circuito permanente CBR para seu destino. Ao mesmo tempo em que se procede à transformação da informação em celas, executa-se um algoritmo de extremo a extremo, que garante o sincronismo do circuito. Este conjunto de procedimentos está documentado no método de adaptação a ATM AAL1.
Mediante a técnica de imitação de circuito, uma rede ATM pode comportar-se como uma rede de transporte baseada na multiplexação no tempo (TDM). Este tipo de serviço permite transportar enlaces digitais de central, linhas ponto a ponto, enlaces E1 para *codecs*, etc. transparentemente.
O objetivo na definição de ATM foi que esta fora a nova geração de rede de transporte de banda larga, com um conjunto de funcionalidades novas, mas completamente compatível com os serviços tradicionais de transporte.

Comutação de voz (VSTN)
Como para o tráfico Frame Relay, ATM oferece uma nova maneira de transportar o tráfico de voz sobre a rede de transporte (a parte da óbvia de imitação de circuito). A aproximação consiste em conseguir que a rede de transporte ATM seja emulada como uma grande central de trânsito (*tandem PBX*). Esta técnica recebe o nome de comutação de voz sobre ATM.

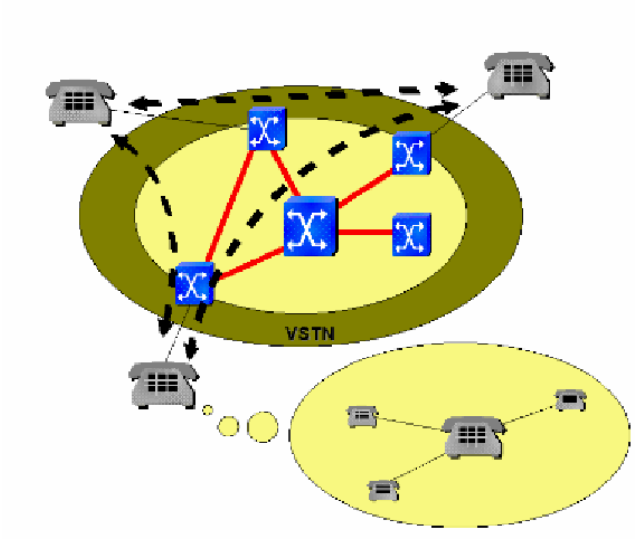


Figura *-Comutação de voz sobre ATM*

O que se procura é que o próprio comutador ATM possa interpretar o canal de sinalização da central e criar canais comutados para a transmissão de cada circuito de voz independentemente. O circuito vai desde a central origem até a de destino sem a necessidade de passar por nenhuma central de trânsito externa.
Ao passo que no caso de FrameRelay, a rede ATM pode conhecer o número de telefonemas de voz que há em cada momento do tempo e, portanto , usar unicamente a largura de banda necessária para sua transmissão (o resto se resigna a outros serviços).
Outras vantagens desta aproximação é a capacidade da rede ATM de informar às centrais pelo canal de sinalização de como prosperam seus telefonemas individualmente. Frente a estas notificações, uma central pode decidir comutar um telefonema determinado pela rede pública em caso de congestão na rede de transporte corporativa. No caso que as centrais usem compressão de voz o uso da técnica de comutação de voz sobre ATM lhes assegura que um determinado circuito se comprime/descomprime num único ponto e, portanto, o sinal não sofre a perda de qualidade associada às redes baseadas em muitos saltos entre centrais.
A comutação de voz sobre ATM elimina a necessidade de grandes centrais de trânsito existentes nas grandes redes de voz e faz mais singelas as tabelas de encaminhamento com o que a Escalabilidade é muito maior (e bem mais econômica).

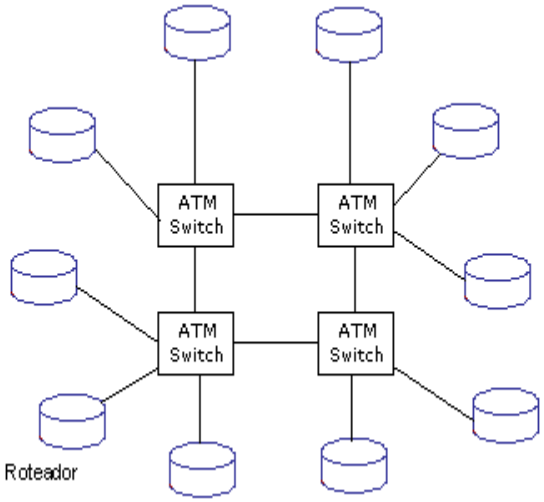
MPLS

MPLS (acrônimo para *Multiprotocol Label Switching*) permite que os operadores de uma determinada rede tenham alto desempenho no desvio de tráfego de dados em situações críticas, tais como de falhas e gargalos (ou congestionamentos). Através do MPLS eles podem assegurar que a transmissão de determinados pacotes tenham perdas ou atrasos imperceptíveis em função da capacidade de uma gestão de tráfego mais eficaz, possibilitando assim maior qualidade dos serviços e conseqüentemente maior confiabilidade. É normalmente utilizado em empresas de Telecomunicações responsáveis por backbones que se utilizam de BGP4, QoS e SLA para

aumentar sua credibilidade quanto à disponibilidade de seus serviços.

Fundamentos

Apesar do IP ter se tornado o protocolo padrão a nível do usuário, as vantagens apresentadas pelas switches em relação aos roteadores, levaram a que a maior parte dos backbones IPs, inclusive da Internet fossem implementados utilizando uma rede ATM no seu núcleo como ilustrado na figura a seguir.



Esta solução apresenta no entanto as seguintes desvantagens:

O mapeamento de pacotes IP no ATM é uma tarefa complexa, tendo sido objeto de vários grupos de estudos.

Esta solução não é escalável. Como cada roteador está, na camada IP (rede), conectado por circuitos virtuais a todos os roteadores conectados ao backbone ATM, pode ser mostrado que a quantidade de informação de roteamento que é transmitida nesta rede no caso de uma mudança de topologia no núcleo da rede pode chegar a ser da ordem de n elevado a quarta potência, onde n é o número de roteadores ao redor do núcleo. Desta forma pode-se chegar a um ponto em que o tráfego com informações de roteamento sozinho pode sobrecarregar o roteador.

IP Switching

Para solucionar estes problemas, a empresa Ipsilon apresentou em 1996 uma arquitetura de rede em que os protocolos de controle do IP rodam diretamente no hardware da switch ATM. As switches ATM ainda encaminham pacotes através da troca de rótulos (label swapping), mas os mecanismos pelos quais eles estabelecem tabelas de encaminhamento e alocam recursos são todos estabelecidos por protocolos de roteamento do IP. Esta solução ficou conhecida com IP switching.

Logo em seguida surgiram outros protocolos dentro desta linha de tecnologia, como o Tag Switching (Cisco) e o ARIS (IBM). O IETF criou então um grupo de trabalho para padronizar uma solução baseada nestes protocolos e que deu origem ao Multiprotocol Label Switching (MPLS).

MPLS

O Multiprotocol Label Switching (MPLS) foi padronizado para resolver uma série de problemas das redes IP, entre eles:

Possibilitar a utilização de switches, principalmente em backbones de redes IP, sem ter de lidar com a complexidade do mapeamento do IP no ATM. Switches são em geral mais baratas e apresentam melhor performance que roteadores.

Escalabilidade

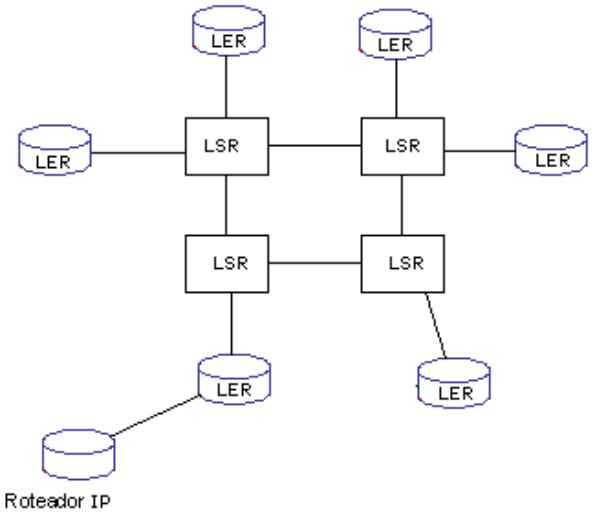
Adicionar novas funcionalidades ao roteamento

O MPLS fornece meios para mapear endereços IP em rótulos simples e de comprimento fixo utilizados por diferentes tecnologias de encaminhamento e chaveamento de pacotes. Este mapeamento é feito apenas uma vez no nó na borda da rede MPLS. A partir daí o encaminhamento dos pacotes é feito utilizando-se a informação contida em um rótulo(label) inserido no cabeçalho do pacote. Este rótulo não traz um endereço e é trocado em cada switch.

O chaveamento de dados a altas velocidades é possível por que os rótulos de comprimento fixo são inseridos no início do pacote e podem ser usados pelo hardware resultando em um chaveamento rápido.

A pesar de ter sido desenvolvido visando redes com camada de rede IP e de enlace ATM, o mecanismo de encaminhamento dos pacotes no MPLS pode ser utilizado para quaisquer outras combinações de protocolos de rede e de enlace, o que explica o nome de Multiprotocol Label switching dado pelo grupo de trabalho do IETF.

Apresenta-se a segui os principais conceitos da arquitetura do MPLS.



Label

Rótulo é um identificador de comprimento curto e definido que é usado para identificar uma FEC, tendo geralmente significado local.

No ATM este rótulo pode ser inserido no cabeçalho da camada de enlace nos campos de VCI ou VPI.

Quando utilizado sobre protocolos onde o cabeçalho da camada de enlace não pode ser utilizado, o rótulo "shim" é inserido entre os cabeçalhos das camadas de enlace e de rede.

Foward Equivalence Class (FEC)

A Foward Equivalence Class (FEC) é a representação de um grupo de pacotes que tem os mesmo requisitos para o seu transporte. Para todos os pacotes neste grupo é fornecido o mesmo tratamento na rota até o seu destino.

FECs são baseados em requisitos de serviço para um dado conjunto de pacotes ou simplesmente por um prefixo de endereçamento.

No roteamento IP convencional um roteador em particular irá tipicamente considerar que dois pacotes estão na mesma FEC pela análise do endereço destino do pacote. Quando o pacote anda na rede, em cada roteador o pacote é re examinado e atribuído a uma FEC.

No MPLS, a atribuição de um pacote particular a uma FEC em particular é feita apenas uma vez, no LER, quando o pacote entra na rede. A FEC atribuída ao pacote é codificada como um valor de comprimento fixo e curto conhecido como "label". Quando o pacote é encaminhado para o próximo roteador o rótulo é enviado juntamente com ele, ou seja o pacote é rotulado antes de ser encaminhado.

Nos roteadores subsequentes (LSR), não existe analise do cabeçalho da camada de rede do pacote. O rótulo é usado como um índice em uma tabela que especifica o próximo roteador e um novo rótulo. O rótulo antigo é trocado pelo novo e o pacote é encaminhado para o próximo roteador.

No MPLS, uma vez que um pacote é associado a uma FEC, não é necessário mais nenhuma análise do cabeçalho por parte dos outros roteadores, todo o encaminhamento é feito a partir dos rótulo.

Label Edge Router (LER)

Um nó MPLS que conecta um domínio MPLS com um nó fora deste domínio.

Label Switching Router (LSR)

O LSR é um nó do MPLS. Ele recebe o pacote de dados, extrai o label do pacote e o utiliza para descobrir na tabela de encaminhamento qual a porta de saída e o novo rótulo. Para executar este procedimento o LSR tem apenas um algoritmo utilizado para todos os tipos de serviço.

A tabela de encaminhamento pode ser única ou existirem várias, uma para cada interface. Elas são compostas utilizando rótulos distribuidos utilizando-se label distribution protocols, RSVP ou protocolos de roteamento como o BGP e OSPF.

Label Distribution Protocol (LDP)

Label Distribution Protocol é um conjunto de procedimentos pelo qual um LSR informa outro das associações entre Label/FEC que ele fez.

Dois LSRs que utilizam um LDP para trocar informações de associações label/FEC são conhecidos como "label distribution peers" em relação a informação de associação que trocaram.

Label Switching Path (LSP)

No MPLS a transmissão de dados ocorre em caminhos chaveados a rótulo (LSPs). LSPs são uma sequência de rótulos em cada e todos os nós ao longo do caminho da origem ao destino. LSPs são estabelecidos antes a transmissão dos dados ou com a detecção de um certo fluxo de dados.

Qualidade de Serviço

A qualidade de serviço em roteamento é a habilidade de escolher o caminho para que um fluxo de tráfego tenha o nível de serviço aceitável. Estes níveis de serviço podem especificar nívies adequados de banda, atrasos ou perda de pacotes na rede. Esta característica agraga inteligência para adminstrar níveis de serviço diferentes de acordo com as políticas da rede.
A habilitação de recursos para um nível de qualidade de serviço desejado requer, na maioria das vezes, rotas explícitas. Pode existir a necessidade de designar uma rota específica para um fluxo de dados que exige uma banda mínima. Entretanto, é possível que as necessidades de usuários em uma rede resultem na utilização combinada (por recursos independentes) da banda de um enlace que exceda a capacidade existente. Esta possibilidade de utilização de recursos da rede requer um nível de granularidade de informações superior ao que pode ser obtido pela engenharia de tráfego tradicional.
Em ambientes MPLS, o tratamento da Qualidade de Serviço para o roteamento é adminstrado de duas formas:
O rótulo MPLS (label) contém informações sobre a Classe de Serviço (CoS). Na medida em que o trafego flui na rede, esta informação é utilizada para priorizar o tráfego em cada nó (hop).
A rede MPLS pode estabelecer múltiplos caminhos entre equipamentos de entrada e saída. Para cada fluxo de informações é estabelecido um nível de serviço apropriado, e o tráfego é direcionado para o caminho adequado quando entra na rede.
Estes procedimentos classificam pacotes em categorias de classes de serviço e as políticas de adminstraçao, nas redes locais, determinam os recursos disponíveis para cada categoria.

Conclusões sobre MPLS
O MPLS proporciona também escalabilidade a rede uma vez que um roteador convencional passa a ter como roteador adjacente o seu LER do Backbone MPLS e não todos os roteadores conectados ao backbone como acontece com backbones ATM.

A utilização de rótulos para encaminhamento de pacotes permite também adicionar novas funcionalidades ao roteamento independentemente do endereço IP na camada de rede. É possível desta estabelecer rotas pré-definidas ou prioridades para pacotes quando da definição das FECs. O MPLS passa a ser portanto uma ferramenta poderosa para implementação de QoS e classes de serviço em redes IP.

Com o MPLS é possível também implementar túneis utilizados na formação de redes privadas virtuais (VPNs). Sendo esta a solução adotada pela maior parte dos provedores de VPN que possuem backbone IP.

SERVIÇOS DE DIRETÓRIOS

X.500

X.500 é um protocolo que especifica um modelo para a conexão de Serviços de Diretórios locais a fim de formar um diretório global distribuído. Os bancos de dados mantêm uma parte do diretório global e sua informação é disponibilizada através de um Agente do Sistema de Diretórios , que se comunica com os outros Agentes do Sistema de Diretórios espalhados pelo mundo. Assim, o usuário, a partir do servidor local, acessa qualquer outro. X.500 suporta, também, funções de gerenciamento, isto é, adição, modificação e deleção de entradas.

Cada entrada no Diretório X.500 descreve um objeto (uma pessoa, uma rede), que tem um identificador único chamado Nome Distinto. Uma entrada consiste de uma coleção de atributos, sendo que, para uma pessoa, estes atributos podem ser nome, endereço, e-mail, etc.

As entradas são encontradas através da navegação na Árvore de Informação do Diretório, que tem em seu topo atributos do "Mundo", sendo a seguir dividida em países e organizações, onde são armazenadas as informações sobre pessoas.

A série de recomendações X.500 define regras para dar nome a objetos, uma Base de Informações de Diretório lógica para guardar informações sobre estes objetos e as entidades de protocolo que cooperam para prover o Serviço de Diretórios.

1.9. 1. Introdução

A necessidade de um serviço de diretórios advém do contraste entre a constante mudança da rede OSI como um todo e da necessidade de isolar (tanto quanto possível) o usuário da rede destas mudanças. Logo, um cliente de um serviço de diretório pode ver a rede OSI como uma entidade mais estável. Por exemplo, se a localização física de um recurso na rede é alterada, o usuário daquele recurso não será afetado pela mudança, desde que esteja usando um nome para referenciá-lo e não um endereço físico.

Outra necessidade para um serviço de diretório advém do desejo de prover uma visão mais ergonômica ("user-friendly") da rede. Por exemplo, o uso de apelidos, o oferecimento de um serviço de "páginas amarelas", ajudam a minorar a dificuldade de encontrar e usar informação na rede.

A CCITT e a ISO definiram um conjunto de padrões para um serviço de Diretório de rede [CCIa88] e [ISOa88]. Tais padrões especificam um sistema de Diretório distribuído que atende a consultas sobre objetos da rede. O Sistema de Diretório assim definido engloba uma base de dados constituída de nomes e, para cada nome, um conjunto de propriedades a serem associadas com aquele nome. Por exemplo, dado o nome de uma pessoa, em forma apropriada, um serviço de Diretório pode devolver um endereço eletrônico ou número de telex. O serviço de Diretório pode ser também usado para apoiar a definição de grupos de objetos, para autenticação de usuários e para funções de gerenciamento de redes, tais como registro da localização de aplicações.

Adicionalmente, além de permitir a seus clientes recuperarem informações, o serviço de Diretório tem mecanismos para atualizar e gerenciar a informação que contém.

Serviços de Diretório X.500

Os serviços de Diretório descritos nessa seção são os serviços que um AUD pode requisitar a um ASD. A série X.500 usa operações remotas como um modelo para solicitação e fornecimento de serviços. Conceitualmente, as operações remotas são muito simples. O iniciador da operação invoca-a a partir de um ponto remoto. O resultado ou uma mensagem de erro e retornado. As operações remotas são definidas em termos de seu objetivo (ou função) e dos parâmetros passados entre seus solicitadores e respondedores.

Cada pedido de serviço contém controles sobre o modo que o Diretório deve processar o pedido. Exemplos de tais controles incluem:

- Filtros que especificam atributos nos quais o Diretório deveria basear a pesquisa. Filtros podem conter expressoes booleanas e operadores de comparação.
- Seletores que controlam quais atributos devem ser recuperados de uma entrada de um objeto. Um seletor pode especificar valores e tipos ou somente tipos e atributos (verficando a presença de um atributo) que devem ser retornados.
- Parâmetros de segurança, incluindo assinatura digital, horario e números aleatórios.

- Limites na extensão de tempo ate que o pedido expire, no número de entradas de objetos que podem ser retornados, na porção do Diretório em que o pedido pode ser processado, na prioridade em que o processamento deve ocorer e nos meios que o ASD pode usar para processar o pedido.

A seguir são descritas as operações que um AUD pode solicitar.

- **Conexão e Desconexão (Binding e Unbinding)** As operações de conexão e desconexão são as primeiras e as últimas numa série de operações que um AUD invoca num ASD. Elas governam o relacionamento operacional entre um AUD e um ASD. A ligação prove um meio para um AUD se identificar a um ASD e vice-versa. O desligar e usado por um AUD para assinalar o fim de uma série de operações.
- **Operações de Leitura** Duas operações ler (READ) e comparar (COMPARE) são usadas para examinar a informação associada com uma entrada de objeto particular. Ler e usado para extrair informação de uma particular entrada ou para verificar um nome único e distinto. Comparar e similar a ler exceto que o AUD fornece informação para o ASD comparar contra uma entrada de objeto.
- **Operações de Pesquisa** Duas operações, listar (LIST) e pesquisar (SEARCH) podem retornar informações sobre múltiplos objetos. Dada uma particular entrada na AID-Árvore de Informações de Diretório, a operação de listar retorna os nomes distintos relativos de suas entradas subordinadas. Dado um conjunto de critérios de seleção, pequisar identifica as entradas de interesse numa sub-árvore na AID e retorna a informação extraída dessas entradas.
- **Operações de Modificação** Três Operações são usadas para manter a informação armazenada nos nodos folhas da AID: adicionar (add) remover (remove) e modificar (modify). Operações de adicionar ou remover criam ou deletam folhas. Modificar pode ser usado para adicionar ou remover atributos de uma entrada folha ou para alterar os valores de atributos de uma entrada folha. O projeto e implementação dos controles de acesso sobre adicionar, remover e modificar são decisões a cargo do implementador.

  Deve ser destacado que ainda não existe qualquer provisão formal para apropriar modificar ou deletar informação armazenada em nos intermediários. A maneira como isto e realizado e assunto local de cada implementação.

- **Operação de Abandono** Abandono (abandon) pode ser invocado por um AUD - Agente de Usuário de Diretório, após uma operação anteriormente invocada, para dizer ao ASD que não há mais interesse nos resultados da mesma. Deve-se notar que o abandono não necessariamente cancela a operação. Cancelar a operação poderia ser difícil de efetuar, dada a natureza distribuída do Diretório.

Protocolos do Diretório

Existem dois protocolos usados pelo Diretório. **Protocolo de Acesso do Diretório (PAD)** é usado em interações entre um AUD e um ASD. O **Protocolo do Sistema de Diretórios (PSD)** é usado em interações entre dois ASD. Ambos os protocolos são baseados no conceito de operações remotas. Todas as interações dos protocolos PAD e PSD são especificadas pelos argumentos passados com a invocação, os argumentos que podem ser retornados com os resultados e as possíveis mensagens de erro.

As operações remotas que um ASD pode invocar em outro ASD são praticamente as mesmas operações remotas que um AUD pode invocar em um ASD.

O Diretório implementa operações remotas usando o elemento serviço de operações remotas (ROSE-Remote Operation Service Element) que e parte do nível de aplicação. As operações de Ligar e desligar (BIND e UNBIND) constituem uma exceção. Elas usam o elemento de serviço de controle de associação (ACSE-association Control Service Element) que e também parte do nível de aplicação. ROSE pode ser implementado diretamente sobre a camada de apresentação ou pode usar os serviços do RTSE-Reliable Transfer Service Element.

1.10. Padrões de uso do Diretório

O serviço de Diretório e definido em termos de um particular pedido que um AUD pode fazer e os parâmetros inerentes. As aplicações que usam o serviço de Diretório porem podem variar seguindo vários padrões, tais como os seguintes:

1.10.1. Pesquisa

A pesquisa pura e simples no Diretório sera provavelmente o tipo mais comum de consulta submetido e envolve a apresentação de um nome distinto de um objeto com um tipo de atributo. O Diretório retornara um valor ou valores correspondentes aquele tipo de atributo. Tipos de atributos de diversas espécies são padronizados (endereços Originador/Destinatário de Sistemas de Mensagens, números de telefone e telex, etc...

A pesquisa e apoiada pelo serviço de leitura e pode ser baseada em outros nomes, além do nome distinto de um objeto, como por exemplo, em seu apelido. Além disso, podem ser requisitados os valores de mais de um atributo.

1.10.2. 5.2 Nomes amigáveis

Podem ser dados nomes mais fáceis de memorizar a objetos. Tais nomes serão possivelmente baseados em atributos que são inerentes ao objeto e serão usados por todas as aplicações que se referirem a ele.

1.10.3. Pesquisa por varredura

Em algumas situações pode ser que o usuário (ou AUD) conheça o nome, o nome amigável etc, mas pode também acontecer que ele apenas seja capaz de reconhecê-lo quando vê-lo. Assim, uma capacidade de busca por varredura ("browsing") permitiria percorrer os dados procurando entradas relevantes. Isto seria efetivado mediante combinação dos serviços de lista e pesquisar, possivelmente em conjunto com a operação de leitura.

Páginas amarelas

Existe uma variedade de meios para prover um serviço do tipo do oferecido nas páginas amarelas. A forma mais simples e baseada em filtros, usando atributos cujos valores são as categorias definidas.

Uma abordagem alternativa e baseada no estabelecimento de sub-árvores especiais cujas estruturas são projetadas especialmente para o serviço de páginas amarelas.

Grupos

Um grupo e um conjunto cujo conteúdo pode variar pela adição ou remoção de membros. O grupo e um objeto, assim como seus membros. O Diretório pode ser solicitado a:

- indicar se um particular objeto e membro de um grupo
- listar a composição de um grupo

Autenticação

Muitas aplicações requerem a apresentação de alguma prova de identidade para permitir a execução de determinadas ações. O Diretório provê suporte para este processo de autenticação alem de requerer ele próprio que seus usuários se identifiquem.

A abordagem mais direta, denominada "autenticação simples" e baseada no Diretório conter um atributo "Senha de Usuário" para uso por aqueles usuários que desejarem ou precisarem da autenticação frente a algum serviço. Por requisição deste serviço, o Diretório confirmará ou não que um particular valor apresentado e realmente a senha do usuário. Isto evita a necessidade de dispor de diferentes senhas para cada serviço.

A abordagem mais complexa, denominada "autenticação forte" e baseada em criptografia com chave pública e o Diretório atua como repositório da chaves de criptografia pública dos usuários. Ha vários passos, descritos na recomendação X.509 [CCIb 88], detalhando os passos que os usuários devem seguir para obter as chaves públicas de outros usuários do diretório e usá-las para autenticar um ou outro.

1.11. Alguns Tipos de Atributos e Classes de Objeto

A X.500 define um certo número de tipos de atributos e classes de objetos que podem ser usados embora não obrigatoriamente.

1.11.1. 6.1 Atributos

A X.520 definiu onze grupos de tipos de atributos:

- Tipos de atributos de sistema denotam a classe de um objeto, um pseudônimo de um objeto, se existe, e uma descrição legível por seres humanos do conhecimento armazenado por um específico ASD (conhecimento de como a BID e distribuída entre os ASDs).
- Tipos de atributo de rotulação são cadeias de caracteres que as pessoas associam com os objetos. Exemplos disso incluem nomes comum, tais como "Joao Silva" ou "Modem de Alta Velocidade" ou números seriais.
- Tipos de atributos geográficos associam uma regiao ou posição geográfica com um objeto. Exemplos incluem país, estado e localidade.
- Tipos de atributos organizacionais identificam a organização em que o objeto e afiliado e o papel do objeto naquela organização tal como nome da organização e cargo.
- Tipos de atributos explanatório fornecem auxílio ao usuário de Diretório. Por exemplo eles podem descrever o objetivo de um objeto, sugerir critério de pesquisa que pode ser útil numa sub-árvore ou dar a ocupação de uma pessoa.
- Tipos de atributo de endereçamento postal especificam a informação requerida para a entrega física de um objeto tal como um nome de rua ou uma caixa postal.
- Tipos de atributos de telecomunicações associam um ou mais endereços eletrônicos com um objeto. Exemplos de tais endereços incluem números de telefones, números de telex números de teletex, números de fac-simile, endereços X.121, endereços RDSI e informação de enderecamento usada para telegramas.
- Tipos de atributos de preferência especificam a ordem prioritária de escolha do método a ser usado na tentativa de comunicar-se com o objeto (por exemplo correio eletrônico, telefone).
- Tipos de atributo de aplicação OSI armazenam o endereço de apresentação e o contexto de aplicação de uma entidade de aplicação OSI.
- Tipos de atributo relacional implementam o conceito de grupos e relacionamentos no Diretório. Exemplos desses atributos incluem

membro, proprietário, papel e "veja outros". Note que a o Diretório não inclui mecanismos explícitos para manter a consistência desta informação.

- Tipos de atributo de segurança suportam mecanismos de autenticação que podem ser usados pelo Diretório. Exemplos deste atributo incluem palavra-senha e certificações.

1.11.2. Classes de Objetos

A X.500 define um conjunto de classe de objetos:

Top (de qual qualquer outra classe e uma sub-classe)
Pseudonimo
Pais
Localidade
Organização
Unidade Organizacional (uma sub-divisão de uma organização)
Pessoa
Pessoa Organizacional (uma sub-classe de pessoa usada no contexto de negocios)
Regra Organizacional (tal como contas a receber)
Grupos de Nomes (podem ser recursivamente definidos)
Pessoa Residencial (uma sub-classe de pessoa usada fora do contexto do comercial)
Processo de Aplicação
Entidade de Aplicação
ASD (Agente do Sistema de Diretório)
Dispositivo

LDAP

Nota: A versão 2.1 do OpenLDAP é agora a versão padrão do LDAP usada no Conectiva Linux. A versão anterior, 1.2.x, é oferecida apenas para compatibilidade com binários antigos, e se chama openldap1-1.2.11.

1.12. Apresentação

LDAP é um protocolo (executado sobre o TCP/IP) cliente-servidor, utilizado para acessar um serviço de Diretório. Ele foi inicialmente usado como uma interface para o X.500, mas também pode ser usado com autonomia e com outros tipos de servidores de Diretório. Atualmente vem se tornando um padrão, diversos programas já têm suporte a LDAP. Livros de endereços, autenticação, armazenamento de certificados digitais (S/MIME) e de chaves públicas (PGP) são alguns dos exemplos onde o LDAP já é amplamente utilizado.

1.12.1. Serviço de Diretório

Um *Diretório* é como um banco de dados, mas tende a conter mais informações descritivas, baseadas em atributo e é organizado em forma de árvore, não de tabela. A informação em um Diretório é geralmente mais lida do que é escrita. Como conseqüência, Diretórios normalmente não são usados para implementar transações complexas, ou esquemas de consultas regulares em bancos de dados, transações estas que são usadas para fazer um grande volume de atualizações complexas. Atualizações em Diretórios são tipicamente simples ou nem são feitas.

Diretórios são preparados para dar resposta rápida a um grande volume de consultas ou operações de busca. Eles também podem ter a habilidade de replicar informações extensamente; isto é usado para acrescentar disponibilidade e confiabilidade, enquanto reduzem o tempo de resposta.

Existem várias maneiras diferentes para disponibilizar um serviço de Diretório. Métodos diferentes permitem que diferentes tipos de informações possam ser armazenadas no Diretório, colocando requerimentos diferentes, sobre como aquela informação poderá ser referenciada, requisitada e atualizada, como ela é protegida de acessos não autorizados, etc. Alguns serviços de Diretório são locais, fornecendo o serviço para um contexto restrito (exemplo: o serviço finger em uma máquina isolada). Outros serviços são globais, fornecendo o serviço para um contexto muito maior (por exemplo, a própria Internet).

Serviços globais normalmente são distribuídos (Figura 5-1), ou seja, cada servidor é responsável por uma parte apenas. O DNS (*Domain Name System*) é um exemplo, ele é um tipo de serviço de Diretório, embora bastante especializado.

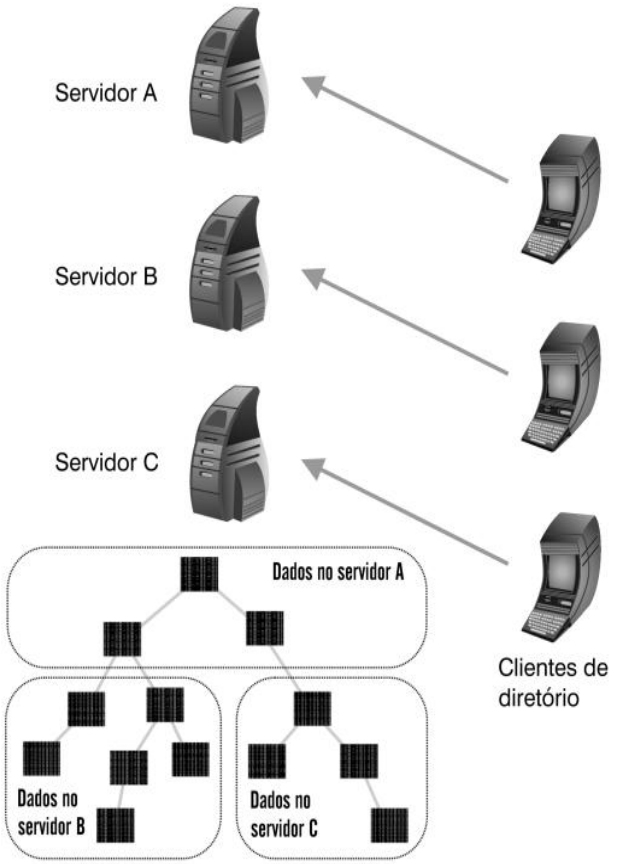


Figura 5-1. Dados de um Diretório distribuídos em três servidores

1.12.2. Tipo de Informação

O modelo de serviço do Diretório LDAP é baseado em **entradas**. Uma entrada é um conjunto de **atributos** e é referenciada através de um **nome distinto**[1]. O DN é usado para referenciar uma entrada de forma não ambígua. Cada um dos atributos de entrada tem um **tipo** e um ou mais **valores**. Este tipos geralmente são palavras mnemônicas, como cn para nome comum, ou mail para endereço de correio eletrônico; existem *RFCs* (*Request For Comments*) que determinam estas palavras. Os valores dependem do tipo de atributo. Por exemplo, um atributo mail pode conter o valor <mari@marilia.br>. Um atributo photoJpeg irá conter uma fotografia.

1.12.3. Organizando a Informação

No LDAP, entradas de Diretório são organizadas em uma hierarquia de árvore invertida, semelhante em alguns aspectos à organização do DNS. A estrutura desta árvore geralmente reflete limites políticos, geográficos e/ou organizacionais. O nó mais alto (**raiz**) é tipicamente o componente nome de domínio **dc**[2] de uma companhia, estado ou organização. Abaixo ficam as entradas representando estados ou organizações nacionais. Abaixo elas podem ser entradas representando pessoas, unidades organizacionais, impressoras, documentos, ou qualquer outra coisa em que você possa pensar. A Figura 5-2 mostra um exemplo de um Diretório LDAP em árvore.

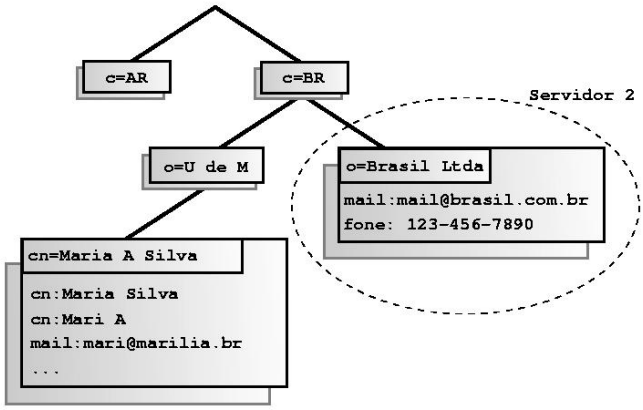


Figura 5-2. Árvore de Diretório LDAP

Apesar de termos entradas para países, o diretório não possui uma entidade centralizadora como, por exemplo, o *root servers* do DNS. A separação por países, por exemplo, pode ser útil para empresas multinacionais. A Figura 5-2 também ilustra uma outra vantagem de um serviço de Diretórios. Os *ramos* da árvore podem estar em máquinas diferentes. No caso da Figura 5-2, a entrada o=Brasil Ltda está em um outro computador. Note que esta característica também é típica do DNS.

1.12.4. Classes de Objetos

Já foi visto alguns tipos de atributos usados nas entradas em um serviço de Diretórios: mail, cn, telephoneNumber e outros. Pode-se criar qualquer tipo de atributo, mas isto não é recomendado. No LDAP existem diversas classes de objetos, e cada classe contém uma lista de atributos obrigatórios e opcionais. Essa lista é tipicamente definida em uma RFC, mas empresas ou organizações também podem criar suas próprias classes.

Por exemplo, a classe *person* é definida da seguinte maneira (definida na RFC2256):

```
objectclass ( 2.5.6.6 NAME 'person' SUP top STRUCTURAL
  MUST ( sn $ cn )
  MAY ( userPassword $ telephoneNumber $ seeAlso $ description ) )
```

O servidor LDAP pode ser configurado para verificar as classes (através da opção *schemacheck*) e forçar o uso correto dos atributos. Isto geralmente é uma boa idéia; com a verificação das classes habilitada, será obrigatória a inserção dos atributos objectClass, sn e cn, por exemplo. Quando for definido que uma entrada do Diretório é da classe *person*, um atributo *description* será opcional. Entradas em Diretórios podem ter várias classes diferentes, basta apenas observar os requisitos de atributos de cada classe.

1.12.5. Referenciando a Informação

Uma entrada é referenciada pelo seu nome distinto DN. O DN é único e na sua construção utiliza o *caminho* inteiro, desde a entrada até o topo do Diretório. Por exemplo, na Figura 5-2, DN="cn=Maria A Silva,o=U de M,c=BR". As entradas também podem ser referenciadas através de um RDN (*Relative Distinguished Name*). Ainda neste exemplo o RDN é cn=Maria A. Silva. Pode-se fazer uma comparação com hostname (RDN) e FQDN (DN).

1.12.6. Acessando a Informação

O LDAP define operações para consultar e atualizar o Diretório. Operações são fornecidas para adição e remoção de uma entrada do Diretório, modificação de uma entrada existente e modificação do nome de uma entrada. A operação LDAP de busca pode abranger a árvore toda (uma busca com escopo *subtree*) ou apenas um ramo, sem *descer* ou *subir* para os demais. Além de especificar com filtros quais entradas se deseja encontrar, também é possível especificar quais atributos destas entradas estão sendo procurados. Se os atributos não forem especificados, todos serão retornados.

Por exemplo, na Figura 5-2 você pode querer pesquisar toda a sub-árvore de Diretório abaixo da Universidade de Marília, procurando por pessoas com o nome de Maria Silva, recuperando o endereço de correio eletrônico para cada entrada encontrada. O LDAP permite que você faça isto facilmente. Ou você pode querer buscar as entradas diretamente abaixo do c=BR, entrada para organizações com a palavra "Brasil" no seu nome, e que tenham um número de telefone. O LDAP permite que você faça isto também. A próxima seção descreve com mais detalhes o que você pode fazer com LDAP e como isto poderá ser útil.

1.12.7. Proteção Contra Acessos Não Autorizados

Alguns serviços de Diretório não fornecem proteção, permitindo que qualquer um possa ver as informações. O LDAP fornece um método para autenticação de um cliente, ou prova sua identidade para um servidor de Diretório, pavimentando o caminho para um rico controle de acesso, protegendo as informações contidas no servidor.

1.12.8. Funcionamento do LDAP

O serviço de Diretório LDAP é baseado em um modelo *cliente-servidor*. Um ou mais servidores LDAP contêm os dados criando a árvore de Diretório LDAP. Um cliente LDAP conecta-se a um servidor e faz uma requisição. O servidor responde com a requisição, ou exibe um ponteiro para um local onde o cliente pode conseguir a informação (tipicamente, outro servidor LDAP). Pode-se fazer novamente uma comparação com o DNS, a diferença é que o servidor LDAP não faz buscas recursivas, ou seja, em nome do cliente. O cliente é encarregado de procurar pelo servidor até encontrar a informação desejada.

1.12.9. Conceito e Utilização do slapd

O *slapd* é um servidor de Diretório LDAP que pode ser executado em diferentes plataformas Linux. Você pode usá-lo para fornecer o seu próprio serviço de Diretório. Seu Diretório pode conter qualquer coisa que você queira colocar. Você pode conectá-lo a um serviço de Diretório LDAP global, ou executar o serviço para você mesmo. Algumas das características e potencialidades mais interessantes do *slapd* incluem:

Escolha do banco de dados: O slapd vem com quatro tipos diferentes de banco de dados que você pode escolher. São eles: LDBM, um banco de dados baseado em disco de alta performance; SHELL, uma interface de banco de dados para comandos arbitrários do Linux ou *scripts* de linha de comando e PASSWD, um banco de dados simples de um arquivo de senhas. A partir da versão 2.1 do OPENLDAP também existe a opção de usar **BDB**[3] como *backend* que é o padrão.

Múltiplas instâncias dos bancos de dados: O *slapd* fornece uma rica e poderosa facilidade no controle de acesso, permitindo a você controlar o acesso a informação em seu(s) banco(s) de dados. Você pode controlar o acesso às entradas baseadas em informação de autenticação LDAP, endereço IP, nome do domínio e outros critérios.

Gerenciamento de processos: O *slapd* utiliza vários processos para ter uma alta performance. Um único sub-processo *slapd* manuseia todas as requisições vindas, reduzindo a quantidade requisitada de recursos do sistema. O *slapd* irá automaticamente selecionar o melhor suporte a vários processos para a sua plataforma.

Replicação: O *slapd* pode ser configurado para usar réplicas. Este esquema de replicação mestre/escravo é vital em ambientes de grande volume, onde um único *slapd* não pode fornecer a disponibilidade ou a confiabilidade necessárias.

Facilidade de configuração: O *slapd* é altamente configurável. Através de um único arquivo de configuração ele permite mudar simplesmente tudo, sempre que você quiser alterar. As opções de configuração têm padrões razoáveis, tornando o seu trabalho muito mais fácil.

As características do openldap-2.1.x são:

LDAPv2 e LDAPv3: O slapd suporta as versões 2 e 3 do LDAP. Ele fornece suporte para as últimas características enquanto mantém interoperabilidade com os clientes existentes. O slapd tem suporte somente ao IPv4. Por padrão, apenas o LDAPv3 está habilitado.

Autenticação SASL: O slapd tem suporte a serviços de autenticação diferenciados através do uso de SASL. A implementação SASL do slapd utiliza o software Cyrus SASL com suporte a vários mecanismos, incluindo DIGEST-MD5 e CRAM-MD5.

Camada de Transporte Segura: O slapd fornece proteções de privacidade e integridade através do uso de TLS. A implementação TLS do slapd utiliza o software OpenSSL[4].

Internacionalização: O slapd suporta Unicode e tags de linguagem.

1.12.10. LDAP e o X.500

O LDAP foi originalmente desenvolvido como um cliente para o X.500, o serviço de Diretório OSI. O X.500 define o Protocolo de Acesso a Diretório (DAP[5]) para os clientes usarem quando estiverem em contato com servidores de Diretório. O DAP é um protocolo pesado, que roda sobre uma camada OSI completa, e precisa de uma quantidade significante de recursos computacionais para ser executado. O LDAP roda diretamente sobre o TCP e fornece a maioria das funcionalidades do DAP, a um custo muito menor.

Este uso do LDAP torna fácil acessar o Diretório X.500, mas ainda exige um serviço X.500 completo, para tornar os dados disponíveis aos vários clientes LDAP que estão sendo desenvolvidos.

Se você já está executando um serviço X.500 e quer continuar a fazer isto, você provavelmente pode parar de ler este capítulo, ele é todo sobre como executar o LDAP via *slapd*, sem utilizar o X.500. Se você não está usando o X.500, quer parar de usar o X.500 ou não tem planos imediatos para executar o X.500, continue lendo.

É possível replicar dados de um servidor de Diretório *slapd* para um DAP X.500; isto permite que sua organização torne seus dados disponíveis como parte de um serviço de Diretório X.500 global em uma base somente para leitura.

Um outro caminho para tornar os dados em um servidor slapd disponíveis para a comunidade X.500 seria usando um DAP X.500 para porta de entrada do LDAP.

1.12.11. Replicação

O slurpd é um servidor para Linux que auxilia o slapd, provendo a replicação do banco de dados. Ele é responsável pela distribuição das mudanças ocorridas no servidor *master* para o servidor *slave* (a réplica). Veja a Figura 5-3.

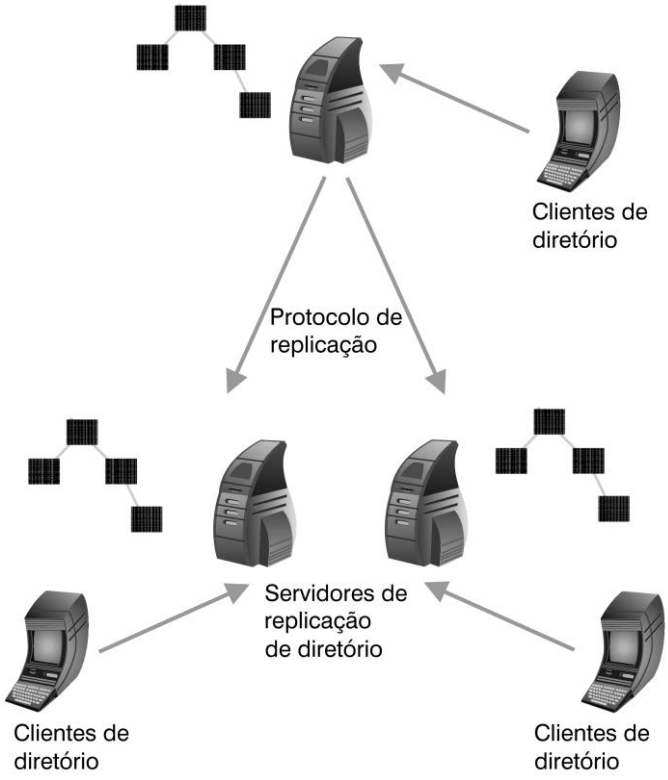


Figura 5-3. Um Serviço de Diretório Replicado com Dados Distribuídos em Três Servidores

O slapd e o slurpd se comunicam através de um simples arquivo texto, que é usado para registrar as mudanças. A sintaxe deste arquivo lembra um pouco a sintaxe dos arquivos resultantes do *diff*, no sentido de que estão descritas as entradas ou atributos que devem ser removidos, adicionados ou modificados. O slurpd irá se encarregar de aplicar estas mudanças ao servidor da réplica. Durante este processo, a réplica e o *master* ficarão diferentes.

Gerenciamento de Redes

INTRODUÇÃO

Até o início da década de 1980, redes de computadores eram baseadas em arquiteturas e protocolos patenteados, a exemplo de System Network Architecture (SNA) da IBM e DECNET da Digital Equipment Corporation.

Já no final da década de 1980, redes interconectadas baseadas na arquitetura e protocolos TCP/IP estavam em franca ascensão. Porém, do ponto de vista da gerência de tais redes, a situação ainda favorecia arquiteturas proprietárias, devido à inexistência de soluções de gerência de redes TCP/IP.

Com o crescimento das redes TCP/IP, aumentaram consideravelmente as dificuldades de gerência. A demora no aparecimento de soluções abertas baseadas no modelo OSI fez com que um grupo de engenheiros decidisse elaborar uma solução temporária baseada num novo protocolo: Simple Network Management Protocol (SNMP). A simplicidade do SNMP facilitou sua inclusão em equipamentos de interconexão. No final da década de

1990, a solução SNMP já era tão difundida que se estabelecera como padrão de gerência de redes de computadores. Hoje, praticamente todos os equipamentos de interconexão dão suporte a SNMP, bem como muitos outros dispositivos (nobreaks, modems etc.), e sistemas de software (servidores Web, sistemas de bancos de dados etc.).

OS PRINCIPAIS OBJETIVOS DO PROTOCOLO SNMP

- Reduzir o custo da construção de um agente que suporte o protocolo;
- Reduzir o tráfego de mensagens de gerenciamento pela rede necessárias para gerenciar dos recursos da rede;
- Reduzir o número de restrições impostas as ferramentas de gerenciamento da rede, devido ao uso de operações complexas e pouco flexíveis;
- Apresentar operações simples de serem entendidas, sendo facilmente usadas pelos desenvolvedores de ferramentas de gerenciamento;
- Permitir facilmente a introdução de novas características e novos objetos não previstos ao se definir o protocolo;
- Construir uma arquitetura que seja independente de detalhes relevantes a somente a algumas implementações particulares.

AGENTE DE GERENCIAMENTO

O agente de gerenciamento é o componente contido nos dispositivos que devem ser gerenciados. Bridges, roteadores, hubs e switches podem conter agentes SNMP que permitem que eles sejam controlados pela estação de gerenciamento. O agente de gerenciamentoresponde à estação de gerenciamento de duas maneiras:

1. **Polling** – A estação de gerenciamento solicita dados ao agente e o agente responde com os dados solicitados.
2. **Interceptação** – É um método de reunião de dados projetado para reduzir o tráfego na rede e para o processamento nos dispositivos que estão sendo monitorados. Em vez da estação de gerenciamento fazer polling nos agentes em intervalos determinados e contínuos, são definidos limites (superiores e inferiores) no dispositivo de gerenciamento. Se esses limites forem ultrapassados no dispositivo, o dispositivo de gerenciamento enviará uma mensagem de alerta à estação de gerenciamento. Isso elimina a necessidade de fazer polling em todos os dispositivos gerenciados na rede. A interceptação é muito útil em redes com muitos dispositivos que precisem ser gerenciados. Ela reduz a quantidade de tráfego SNMP na rede para fornecer mais largura de banda para a transferência de dados.

O mundo SNMP está baseado em três documentos:

- Structure of Management Information (SMI). Definido pela RFC 1155, a SMI traz essencialmente, a forma pela qual a informação gerenciada é definida.
- Management Information Base (MIB) principal. Definida na RFC 1156, a MIB principal do mundo SNMP (chamada MIB-2) define as variáveis de gerência que todo elemento gerenciado deve ter, independentemente de sua função particular. Outras MIBs foram posteriormente definidas para fins particulares, tais como MIB de interfaces Ethernet, MIB de nobreaks, MIB de repetidores etc.
- Simple Network Management Protocol (SNMP). Definido pela RFC 1157, é o protocolo usado entre gerente e agente para a gerência, principalmente trocando valores de variáveis de gerência.

MENSAGENS NO PROTOCOLO SNMP

Ao contrário de muitos outros protocolos TCP/IP, as mensagens no protocolo SNMP além de não apresentarem campos fixos, são codificadas usando a sintaxe ASN.1 (tanto a mensagem de pedido, como a de resposta) o que dificulta o entendimento e a decodificação das mensagens.

Os cinco tipos de mensagens SNMP são:
_ get-request-PDU: mensagem enviada pelo gerente ao agente solicitando o valor de uma variável;
_ get-next-request-PDU: mensagem utilizada pelo gerente para solicitar o valor da próxima variável depois de uma ou mais variáveis que foram especificadas;
_ set-request-PDU: mensagem enviada pelo gerente ao agente para solicitar que seja alterado o valor de uma variável
_ get-response-PDU: mensagem enviada pelo agente ao gerente, informando o valor de uma variável que lhe foi solicitado;
_ trap-PDU: mensagem enviada pelo agente ao gerente, informando um evento ocorrido.
As partes mais importantes de uma mensagem são: as operações (GET, SET e GET-NEXT) e a identificação, no formato ASN.1, dos objetos em que as operações devem ser aplicadas.
Deve existir um cabeçalho que informe o tamanho da mensagem, que só será conhecido após a representação de cada campo ter sido computada. Na verdade, o tamanho da mensagem depende do tamanho de sua parte remanescente (que contém os dados), portanto o tamanho só poderá ser computado após a construção da mensagem. Uma maneira de evitar este problema é construir a mensagem de trás para frente.
Uma mensagem SNMP deve definir o servidor do qual obtemos ou alteramos os atributos dos objetos, e que será responsável por converter as operações requisitadas em operações sobre as estruturas de dados locais. Após verificar os campos de uma mensagem, o servidor deve usar as estruturas internas disponíveis para interpretar a mensagem e enviar a resposta da operação ao cliente que requisitou o pedido. Uma mensagem é constituída por três partes principais:

- A versão do protocolo;
- A identificação da comunidade, usada para permitir que um cliente acesse os objetos gerenciados através de um servidor SNMP;

- A área de dados, que é dividida em unidades de dados de protocolo (Protocol Data Units - PDUs). Cada PDU é constituída ou por um pedido do cliente, ou por uma resposta de um pedido (enviada pelo servidor).

O primeiro campo de uma mensagem SNMP é um operador seqüencial, seguido por um campo com o tamanho total da mensagem (se este tamanho não for igual ao do datagrama, será retornado um código de erro). O próximo campo é um número inteiro que identifica a versão do protocolo SNMP, seguido por um campo usado para a autentificação, indicando a comunidade que o cliente pertence (a comunidade public permite a qualquer cliente acessar os objetos, não precisando o servidor verificar se o cliente pode ou não acessar o objeto). O quarto campo contém a operação que será executada, devendo ser um GET, SET ou GETNEXT pois a operação de TRAP só é gerada pelo servidor. O quinto campo é usado para o servidor ter certeza de que o valor deste campo é igual ao tamanho da parte da mensagem que contém os dados. O sexto campo é uma identificação para o pedido, e o sétimo e o oitavo campos são flags que indicam erros quando estão setadas (campos de status e de índice de erro).
Na definição de uma mensagem, cada uma das PDUs são constituídas ou por um dos cinco tipos de PDUs para as operações ou por uma PDU para a resposta. Na definição da mensagem SNMP, deve-se ter uma sintaxe individual para cada um das cinco operações da PDU. Alguns termos encontrados nas sintaxes das PDUs das operações são:

- O campo RequestID é um inteiro de 4 bytes (usado para identificar as respostas);
- Os campos ErrorStatus e ErrorLevel são inteiros de um byte (sendo nulos em um pedido de um cliente);
- O campo VarBindList é uma lista de identificadores de objetos na qual o servidor procura os nomes dos objetos, sendo definida como uma sequência de pares contendo os nomes dos objetos (em ASN.1 este par é representado como uma sequência de dois itens). Na sua forma mais simples (com um objeto) apresenta dois itens: o nome do objeto e um ponteiro nulo.

LIMITAÇÕES DE SNMP

- Falta de segurança
- Esquema de autenticação trivial
- Limitações no uso do método SET
- Ineficiência
- Esquema de eventos limitado e fixo
- Operação baseada em pooling
- Comandos transportam poucos dados
- Falta de Funções Específicas
- MIB com estrutura fixa
- Falta de comandos de controle
- Falta de comunicação entre gerenciadores
- Não Confiável
- Baseado em UDP/IP
- Trap sem reconhecimento

SNMPV2 E SNMPV3
Visando obter melhorias com relação aos aspectos de segurança foram desenvolvidas novas versões do SNMP. A segunda versão, o SNMPv2 contém mecanismos adicionais para resolver os problemas relativos á segurança como: privacidade de dados, autenticação e controle de acesso.
A terceira versão, o SNMPv3 tem como objetivo principal alcançar a segurança, sem esquecer-se da simplicidade do protocolo, através de novas funcionalidades como:

- Autenticação de privacidade
- Autorização e controle de acesso
- Nomes de entidades
- Pessoas e políticas
- Usernames e gerência de chaves
- Destinos de notificações
- Relacionamentos proxy
- Configuração remota

Como o protocolo SNMP é amplamente utilizado, seria impossível imaginar uma referência rede sem o uso de ferramenta que o implementa. Os mecanismos oferecidos pelo protocolo SNMP permitem efetuar tarefas de monitoração; além da possibilidade de efetuar configuração nos equipamentos gerenciados.
Com o surgimento das novas versões o SNMPv2 e SNMPv3, foram realizadas alterações na especificação do protocolo, tais como a forma de representação das variáveis, e inclusão de novos tipos de PDUs e o retorno dos tipos de erros, que acabaram por tirar a simplicidade do protocolo. Entretanto, o SNMP é amplamente usado, sendo que, a maioria dos fabricantes de hardware para internet (como bridges e roteadores) projetam seus produtos para suportar o SNMP.

Estudo Sobre Cmip

Os modelos predominantemente usados no gerenciamento de redes são o SNMP e o CMIP.
Entretanto, o SNMP foi proposto para gerenciamento de redes internet, mas não vem suportando a complexidade que as redes atuais vem exigindo. E o CMIP proposto pela ISO é muito complexo e seu processo de padronização é muito lento, por isso ele não tem a mesma aceitação do SNMP.

Introdução
O CMIP é um protocolo de gerenciamento definido segundo o padrão OSI. Da mesma maneira que o SNMP, o CMIP especifica como vai ser realizada a troca de informações entre o gerente e o agente no Sistema de Gerenciamento, ou seja, com o primeiro acessando e mudando informações que se encontram na MIB. Os tipos de informação a serem trocadas levam em conta o CMIS (Common management information service), que especifica o conjunto de serviços a que os sistemas gerenciador e gerenciado poderão acessar para que seja realizado o gerenciamento. Juntos CMIS e CMIP formam o que é chamado de CMISE (Common Management Information Service Element), que e uma aplicação da camada 7 do RM-OSI.

O CMISE utiliza duas aplicações de serviço comuns (São aplicações de serviço comum àquelas aplicações que oferecem serviços não só as aplicações de gerenciamento, bem como a todas as outras.), ACSE e ROSE. A primeira trata do estabelecimento e liberação de conexões entre um equipamento e outro. A segunda oferece serviços de requisição de operações remotas.
O CMIP possui onze informações para a troca de mensagens. São elas:

- m-event-report,
- mevent-report-confirmed,
- m-get,
- m-linked-reply,
- m-cancel-get-confirmed,
- m-set,
- m-setconfirmed,
- m-actin,
- m-action-confirmed,
- m-create
- m-delete.

O Protocolo CMIP
Num ambiente de gerenciamento OSI, o protocolo CMIP é utilizado para definir as regras de comunicação entre os processos gerente e agente. Este protocolo trabalha no Nível de Aplicação e é orientado a conexão utilizando os serviços providos pelo ASCE (Association Control Service Element), ROSE (Remote Operations Service Element) e pelo serviço de apresentação.
A utilização dos padrões da ISO para gerenciamento tem sido sustentada pela OSF, que está comprometida, através do OSF/DME (Open Software Foundation/Distributed Management Environment), em suportar os padrões OSI de gerenciamento. A função do DME é fornecer facilidades que permitam integrar o gerenciamento de sistemas em ambientes heterogêneos, satisfazendo três requisitos básicos: interoperabilidade, consistência e flexibilidade.
Da mesma maneira que o SNMP, o CMIP especifica como vai ser realizada a troca de informações entre o gerente e o agente no Sistema de Gerenciamento, ou seja, com o primeiro acessando e mudando informações que se encontram na Mib. Os tipos de informação a serem trocadas levam em conta o serviço do CMIS (Common management information service), que especifica o conjunto de serviços a que os sistemas gerenciador e gerenciado poderão acessar para que seja realizado o gerenciamento.
Juntos CMIS e CMIP formam o que é chamado de CMISE (Common Management information Service Element). Os serviços do CMIS e o protocolo CMIP são usados para implementar sistemas desenvolvidos para vários propósitos, como o gerenciamento de desempenho, de nível de falhas, de segurança, de configuração e de contabilidade, usando os recursos de uma rede baseada no modelo de comunicação OSI.

CMIS
Como já foi dito, o CMIS é uma norma que define o conjunto de serviços oferecidos às aplicações de gerenciamento (software do gerente e software do agente).

O conjunto de serviços oferecidos se enquadram em três categorias. São eles:

- Serviços de Associação: São utilizados para que os usuários do CMIS possam estabelecer as associações necessárias para a realização da comunicação entre si. Para que isso ocorra, no entanto, o CMISE precisa dos serviços oferecidos pela aplicação ACSE.
- Serviços de Notificação: Os serviços de notificação de gerenciamento são utilizados para que o agente sinalize sobre a ocorrência de eventos nos dispositivos gerenciados.
- Serviços de Operação: Os serviços de operação de gerenciamento são utilizados para que o gerente possa obter informações ou alterar as variáveis do MIB.
- Os serviços podem ser confirmados ou não-confirmados. Serviço confirmado significa que quem começou a comunicação (gerente ou agente) deve receber uma resposta vinda do outro lado sobre o sucesso ou o erro da requisição.

Relação de Serviços e PDU's do CMIS/P:
Cada serviço, além de estar enquadrado em uma categoria, está associado a um conjunto de PDU's, exceto os serviços de associação. Abaixo a lista de serviços de acordo com a categoria, ou seja, as 11 PDUs que o CMIP utiliza:

Serviços de Associação:
A-ASSOCIATE:
A-RELEASE:
A-ABORT :

Serviços de Notificação:
M-EVENT-REPORT:

Serviços de Operação:
M-GET
M_CANCEL-GET
M-SET
M-ACTION
M-CREATE
M-DELETE:
M-CANCEL-GET-CONFIRMED

Além das funções apresentadas o CMIS apresenta facilidades adicionais que permitem selecionar um conjunto de objetos sobre o qual pode-se aplicar a mesma operação, e também a existência de respostas múltiplas para cada requisição (uma para cada objeto gerenciado).

São três as facilidades adicionais:
1. **Scopping** - permite selecionar um grupo de instâncias de objetos gerenciados sobre o qual será aplicada uma única operação;
2. **Filtro** - dá a possibilidade de definir um conjunto de testes que serão aplicados a um grupo de instâncias de um objeto, selecionado por uma operação de scopping anterior, permitindo formar um grupo menor a partir deste, sobre o qual as operações de gerenciamento devem ser aplicadas;

3. **Sincronização** permite sincronizar várias operações de gerenciamento a serem aplicadas a instâncias de objetos gerenciados, obtidos através do uso das operações de scopping e de filtragem.

CMISE
O CMISE (Common Management Information Service Element) implementa os serviços definidos pelo CMIS, executando o protocolo CMIP. É correspondente ao mecanismo SASE (Special Application Service Element) da camada de aplicação, e utiliza os elementos ACSE (Association Control Service Element) e ROSE (Remote Operations Service Element) que juntos correspondem ao mecanismo de CASE (Common Application Service Element) também da camada de aplicação.
Os serviços oferecidos pelo CMISE ao protocolo CMIP podem ser confirmados ou não confirmados. A tabela mostra a relação entre os serviços CMISE e as classes de operação do protocolo CMIP. Estes serviços serão mapeados em operações aplicadas sobre os objetos gerenciados, que representam os recursos da rede a serem gerenciados.

SERVIÇO TIPO CLASSE DE OPERAÇÃO
M-EVENT-REPORT confirmado/não-confirmado 2 ou 1/5
M-GET confirmado 2 ou 1
M-CANCEL-GET confirmado 2 ou 1
M-SET confirmado/não-confirmado 2 ou 1/5
M-ACTION confirmado/não-confirmado 2 ou 1/5
M-CREATE confirmado 2 ou 1
M-DELETE confirmado 2 ou 1

CMOT
Existe uma terceira proposta chamada de CMOT (CMIP Over TCP/IP) cujo objetivo é permitir o uso do CMIP em redes com o protocolo TCP/IP.
CMOT (CMIP over TCP/IP) e a utilização do protocolo CMIP dentro da arquitetura internet.
Para que isto seja realizado se faz necessária a implantação do protocolo LPP na camada apresentação da Arquitetura Internet. Este protocolo soluciona eventuais incompatibilidades entre as duas arquiteturas (OSI x INTERNET) no que diz respeito a gerenciamento.

Conceitos básicos
O gerenciamento no modelo OSI da ISO baseia-se na teoria da orientação a objetos. O sistema representa os recursos gerenciados através de entidades lógicas chamadas de objetos gerenciados. Ao desenvolver uma aplicação de gerenciamento, usamos processos distribuídos conhecidos como gerentes (os quais gerenciam) e agentes (os que realizam as ações). Além de definir um modelo informacional, define-se também um modelo funcional em que para cada área é definido um conjunto de funções, que ao serem implementadas, serão usadas para gerenciar a rede. Existem cinco áreas funcionais no gerenciamento num ambiente OSI:

- Gerência de configuração (estado da rede);
- Gerência de desempenho (vazão e taxa de erros);
- Gerência de falhas (comportamento anormal);
- Gerência de contabilidade (consumo de recursos);
- Gerência de segurança (acesso);

Gerentes, agentes e objetos gerenciados
Num ambiente de gerenciamento OSI, usa-se o protocolo CMIP para definir as regras de comunicação entre os processos gerente e agente. O protocolo CMIP implementa as primitivas oferecidas pelo serviço de informação de gerenciamento CMIS. Este ambiente também propõe uma estrutura de gerenciamento para permitir a definição dos conceitos necessários à construção de classes de objetos gerenciados, os princípios necessários à nomeação dos objetos e dos seus componentes, e como é definido o inter-relacionamento entre os objetos. Para descrever a estrutura, são usadas a Hierarquia de Herança, a Hierarquia de Nomeação e a Hierarquia de Registro.

a. Na Hierarquia de Herança a modelagem é realizada com base nas classes de objetos. Parase obter sub-classe com um comportamento mais particular, deve-se detalhar uma superclasse, gerando a partir destas subclasses para um propósito mais particular do que esta classe.
b. Na Hierarquia de Nomeação é descrita a relação de composição entre os objetos, ou seja, a relação de subordinado x superior entre estes objetos, além de serem definidas as regras usadas para nomear os objetos (name binding), de forma que este seja univocamente determinado.
c. Na Hierarquia de Registro são registradas as definições das classes dos objetos, os atributos dos objetos, as ações que podem ser aplicadas, as notificações geradas e os pacotes, seguindo as regras definidas pela notação ASN.1.

SNMP X CMIP
Uma comparação entre o SNMP e o CMIP demonstra que o SNMP é excessivamente simples quando usado em aplicações que não foram previstas quando foi definido, e que apresenta deficiências em relação a segurança ao ser usado em aplicações mais críticas. Já o CMIP é um protocolo poderoso e abrangente que foi concebido com o objetivo de adequar-se à complexidade das redes. Mas apesar desta característica, ainda não alcançou um grau de estável de aceitação pela comunidade. As projeções de mercado demonstram que o SNMP continuará sendo muito usado em pequenas redes, enquanto que o CMIP deve dominar o mercado composto pelas grandes redes corporativas e redes públicas de telecomunicações.
Tanto o SNMP como o CMIP suporta a mesma idéia de troca de mensagens entre gerente e agente e armazenamento das informações na MIB.
O SNMP é simples e mais fácil de ser implementado. Em compensação, possui limitações de desempenho que o CMIP não possui. Principalmente na área de segurança. Portanto o SNMP se adequa mais a sistemas de pequeno porte, pois se pode exigir menos de um sistema de gerenciamento. Devido o CMIP ser bem completo e projetado é mais útil em sistemas de comunicação de grande porte onde existem grandes quantidades de recursos a serem gerenciados. Em contraposição, em sistemas de pequeno porte, ele não se torna adequado devido a sua complexidade.

ESTUDO SOBRE SMI

A SMI descreve o cenário no qual a Base de Informação Gerencial pode ser definida. A SMI, baseada na abordagem orientada a objetos, introduz os conceitos de hierarquia, herança, nomeação e registros usados na caracterização e identificação de objetos gerenciados. Além disso, ela define o conjunto de operações que pode ser realizado sobre os objetos gerenciados da MIB e o comportamento desses objetos mediante a execução destas operações.

Introdução

A SMI (Structure of Management Information), como é chamada esta instrumentação, é análoga à linguagem de programação usada para construir estruturas de dados e permitir operações que possam ser executadas sobre essas estruturas. A combinação de uma SMI com um protocolo particular é denominada framework. Tem por finalidade ser um padrão da MIB e pode ser definida e construída na RFC 1511. Ela identifica os tipos de dados que podem ser utilizados na MIB e especifica como os recursos são reapresentados e nomeados. A SMI procura a simplicidade e a escalabilidade.

DEFINIÇÕES PARA SMI

Um objeto gerenciador não tem apenas que estar definido mas identificado também. Isto é feito usando o Identificador de Objetos como um número de telefone, reservando um grupo de números para diferentes localizações. No caso do TCP/IP - baseado em gerenciamento de rede, o número alocado é 1.3.6.1.2 e a SMI usa isto como uma base para definir novos objetos. Abaixo está um exemplo que mostra a definição de um objeto contido em uma MIB.
Seu nome é sysDescr e faz parte do grupo System.

OBJETO
sysDescr { system 1 }
Sintaxe STRING de OCTETOS
Os tipos de dados SMI são divididos em três categorias:
_ tipo simples
_ tipo de grandes aplicações
_ tipo construtor simples

Os tipos simples incluem quatro tipos ASN. 1 primitivos:

- **Inteiros** - valores negativos ou positivos de todos os números, inclusive o zero
- **Cadeia de octetos** - seqüência ordenada de zero ou mais octetos
- **Identificadores de objetos** – conjunto de todos os identificadores de objetos alocados de acordo com as regras especificadas pelo ASN.1.

Tipos de dados de grandes aplicações referem-se aos tipos de dados especiais definidos pelo SMI:

- **Endereços de rede** - representam um endereço de uma família particular de protocolos
- **Contadores** - inteiros não negativos são incrementados de um em um até atingirem um valor máximo, quando eles são resetados e voltam a zero. O número total de bits recebidos em uma interface é um exemplo de contador
- **Medidas** – inteiros não negativos que são incrementados ou decrementados, porém atrelados a um valor máximo. O tamanho da fila de saída de pacotes é um exemplo.
- **Checagem de tempo** – o tempo de um evento. O tempo necessário para uma interface chegar ao estado corrente é um exemplo
- **Opaco** - representa uma codificação arbitrária. Este tipo de dados é usado para passar uma cadeia de informações arbitrárias que não está de acordo com a tipagem de dados usada no SMI
- **Inteiros** - representa uma informação com valores inteiros sinalizados. Este tipo de dados redefine o tipo de dados simples "inteiro" do ASN.1, que tem uma precisão arbitrária no ASN.1, porém uma precisão determinada no SMI
- **Inteiros sem sinal** – representa uma informação com valores inteiros não sinalizados. Ele é útil quando os valores são sempre não negativos. Este tipo de dados redefine o tipo de dados simples "inteiro" do ASN.1, que tem uma precisão arbitrária no ASN.1, porém uma precisão determinada no SMI.

O tipo construtor simples inclui dois tipos ASN.1 que definem múltiplos objetos em tabelas e listas:

- Linha - referência a uma linha de uma tabela. Cada elemento de uma linha pode ser um tipo simples ou um tipo de grandes aplicações
- Tabela - referência a uma tabela com zero ou mais linhas. Cada linha pode ter um número qualquer de colunas.

A especificação BER, definida por [8825,Specification of Basic Encoding Rules for ASN.1], permite que máquinas diferentes troquem informações de gerenciamento especificando a posição de cada bit nos octetos transmitidos e a estrutura dos bits. A estrutura de bits é definida pela descrição do tipo de dados, tamanho e valor.

Concluímos que a SMI descreve o cenário no qual a Base de Informação Gerencial pode ser definida. A SMI, baseada na abordagem orientada a objetos, introduz os conceitos de hierarquia, herança, nomeação e registros usados na caracterização e identificação de objetos gerenciados. Além disso, ela define o conjunto de operações que pode ser realizado sobre os objetos gerenciados da MIB e o comportamento desses objetos mediante a execução destas operações. A MIB é uma base de dados, cuja estrutura é especificada pelo padrão SMI, como já descrito anteriormente. Ela pode ser caracterizada como um banco de dados ativo, o que possibilita que os valores das suas variáveis sejam, não só recuperados,como também alterados. Cada agente deve manter sua própria instancia da MIB, relacionada com os objetos que estão sendo gerenciados sob o seu domínio. O RFC 1213 define um conjunto de variáveis utilizadas para a monitoração e o controle de redes TCP/IP.

ESTUDO SOBRE MIB

O conhecimento das MIB's (Base de Informações Gerenciáveis), e principalmente, o conhecimento de como

utilizar estas informações são de fundamental importância na Gerência de Redes.

Introdução
Este hiperdocumento procura introduzir o conceito de MIB e apresentar os dois principais padrões de MIB, a MIB da OSI e a MIB da Internet, aprofundando mais neste último, no qual serão apresentados todos os objetos gerenciados e suas possíveis utilizações. Dentro deste contexto, a MIB é definida como um conjunto de objetos gerenciados dentro de um Sistema Aberto, na qual um objeto gerenciado é a visão abstrata de um recurso real dentro deste sistema.

DEFINIÇÃO DE MIB
Antes de definir o que é uma MIB, introduziremos o conceito de objetos gerenciados. Um objeto gerenciado é a visão abstrata de um recurso real do sistema. Assim, todos os recursos da rede que devem ser gerenciados são modelados, e as estruturas dos dados resultantes são os objetos gerenciados. Os objetos gerenciados podem ter permissões para serem lidos ou alterados, sendo que cada leitura representará o estado real do recurso e, cada alteração também será refletida no próprio recurso. Dessa forma, a MIB é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede.

O que é a MIB ?
A MIB é o conjunto dos objetos gerenciados, que procura abranger todas as informações necessárias para a gerência da rede, possibilitando assim, a automatização de grande parte das tarefas de gerência.

MIB DA OSI
O padrão OSI define três modelos para gerência de redes: o modelo organizacional, o modelo informacional e o modelo funcional. O modelo organizacional descreve a forma pela qual a gerência pode ser distribuída entre domínios e sistemas dentro de um domínio. O modelo funcional descreve as áreas funcionais e seus relacionamentos. Já o modelo informacional provê a base para a definição de objetos gerenciados e suas relações, classes atributos, ações e nomes.
Na definição de objetos gerenciados é utilizada a orientação a objetos. Objetos com características semelhantes são agrupados em classes de objetos. Uma classe pode ser uma subclasse de outra, e a primeira herda todas as propriedades da segunda. Uma classe é definida pelos atributos da classe, pelas ações que podem ser invocadas, pelos eventos que podem ser relatados, pela subclasse a qual ela deriva e pela superclasse na qual ela está contida.
Para a definição dos objetos gerenciados deve-se considerar três hierarquias: hierarquia de herança, de nomeação e de registros usados na caracterização e identificação de objetos gerenciados.
A seguir descreveremos cada uma das hierarquias mencionadas acima.
a) **Hierarquia de Herança** – Também denominada hierarquia de classe, tem como objetivo facilitar a modelagem dos objetos.

b) **Hierarquia de Nomeação –** descreve a relação de "estar contido em" aplicado aos objetos. Um objeto gerenciado está contido dentro de um e somente um objeto gerenciado.
Um objeto gerenciado existe somente se o objeto que o contém existir, e dependendo da definição, um objeto só pode ser removido se aqueles que lhe pertencerem forem removidos primeiro.

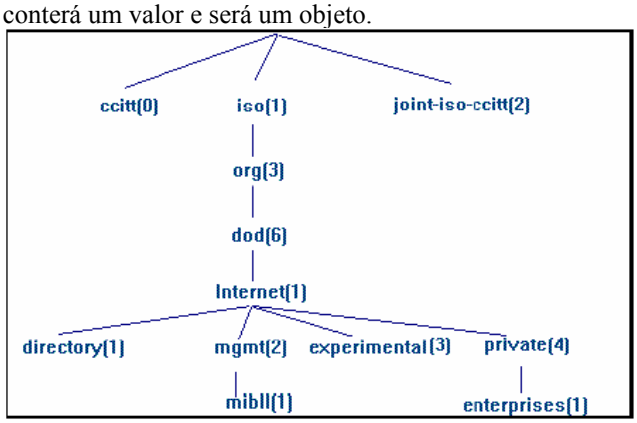
c) **Hierarquia de Registro** – é usada para identificar de maneira universal os objetos, independentemente das hierarquias de heranças e nomeação.

MIB DA INTERNET
A MIB II usa uma arquitetura de árvore, definida na ISO ASN.1, para organizar todas as suas informações. Cada parte da informação da árvore é um nó rotulado que contém:

- um identificador de objetos (OID): seqüência de números separados por pontos.
- uma pequena descrição textual: descrição o nó rotulado

Exemplo:
directory(1)
identificador de objetos: 1.3.6.1.1
descrição textual: {internet 1}

Um nó rotulado pode ter árvores contendo outros nós rotulados. Caso não tenha árvores, ou nós folhas, ele conterá um valor e será um objeto.



O nó raiz da árvore MIB não tem nome ou número, mas tem três árvores:
1. ccitt(0), administrada pelo CCITT
2. iso(1), administrada pela ISO
3. joint-iso-ccitt(2), administrada pela ISO juntamente com o CCITT.

Sob o nó iso(1), estão outras árvores, como é o caso da árvore org(3), definida pela ISO para conter outras organizações. Uma das organizações que está sob a árvore org(3) é o Departamento de Defesa dos EUA (DOD), no nó dod(6). A Internet(1) está sob o dod(6), e possui quatro subárvores:

- directory(1): contém informações sobre o serviço de diretórios OSI (X.500)
- mgmt(2): contém informações de gerenciamento, é sob esta subárvore que está o nó da mibII, com o identificador de objeto 1.3.6.1.2.1 ou {mgmt 1}.

- experimental(3): contém os objetos que ainda estão sendo pesquisados pela IAB.
- private(4): contém objetos definidos por outras organizações.

Abaixo da subárvore mibII estão os objetos usados para obter informações específicas dos dispositivos da rede. Esses objetos são divididos em 11 grupos, que são apresentados na tabela abaixo.

Grupo	Informação
system (1)	informações básicas do sistema
interfaces (2)	interfaces de rede
at (3)	tradução de endereços
ip (4)	protocolo ip
icmp (5)	protocolo icmp
tcp (6)	protocolo tcp
udp (7)	protocolo udp
egp (8)	protocolo egp
transmission (10)	meios de transmissão
snmp (11)	protocolo snmp

Exemplos
Alguns dos objetos pertencentes aos grupos da MIB II são:

Grupo System (1.3.6.1.2.1.1)

- **sysDescr (1.3.6.1.2.1.1.1):** Descrição textual da unidade. Pode incluir o nome e a versão do hardware, sistema operacional e o programa de rede.
- **sysUpTime (1.3.6.1.2.1.1.3):** Tempo decorrido (em milhares de segundos) desde a última re-inicialização do gerenciamento do sistema na rede.
- **sysContact (1.3.6.1.2.1.1.4):** Texto de identificação do gerente da máquina gerenciada e como contatá-lo.

Grupo Interfaces (1.3.6.1.2.1.2)

- _ ifNumber (1.3.6.1.2.1.2.1): Número de interfaces de rede (não importando seu atual estado) presentes neste sistema.
- _ ifOperStatus (1.3.6.1.2.1.2.2.1.8): Estado atual da interface.
- _ ifInOctets (1.3.6.1.2.1.2.2.1.10): Número total de octetos recebidos pela interface.

Grupo IP (1.3.6.1.2.1.4)

- _ ipForwarding (1.3.6.1.2.1.4.1): Indica se esta entidade é um gateway.
- _ ipInReceives (1.3.6.1.2.1.4.3): Número total de datagramas recebidos pelas interfaces, incluindo os recebidos com erro.
- ipInHdrErrors (1.3.6.1.2.1.4.4): Número de datagramas que foram recebidos e descartados devido a erros no cabeçalho IP.

Grupo ICMP (1.3.6.1.2.1.5)

- _ icmpInMsgs (1.3.6.1.2.1.5.1): Número total de mensagens ICMP recebidas por esta entidade. Incluindo aquelas com erros.
- _ icmpOutMsgs (1.3.6.1.2.1.5.14): Número total de mensagens ICMP enviadas por esta entidade. Incluindo aquelas com erros.

Grupo TCP (1.3.6.1.2.1.6)

- tcpMaxConn(1.3.6.2.1.6.4): Número máximo de conexões TCP que esta entidade pode suportar.
- tcpCurrentEstab (1.3.6.2.1.6.9): Número de conexões TCP que estão como estabelecidas ou a espera de fechamento.
- tcpRetransSegs (1.3.6.2.1.6.12): Número total de segmentos retransmitidos.

Grupo UDP (1.3.6.1.2.1.7)

- udpInDatagrams (1.3.6.1.2.1.7.1): Número total e datagramas UDP entregues aos usuários UDP.
- udpNoPorts (1.3.6.1.2.1.7.2): Número total de datagramas UDP recebidos para os quais não existia aplicação na referida porta.
- udpLocalPort (1.3.6.1.2.1.7.5.1.2): Número da porta do usuário UDP local.

Grupo SNMP (1.3.6.1.2.1.11)

- snmpInPkts (1.3.6.1.2.1.11.1): Número total de mensagens recebidas pela entidade SNMP.
- snmpOutPkts (1.3.6.1.2.1.11.2): Número total de mensagens enviadas pela entidade SNMP.
- snmpInTotalReqVars (1.3.6.1.2.1.11.13): Número total de objetos da MIB que foram resgatados pela entidade SNMP.

Comparação Entre A MIB Da OSI E A Mib Da Internet

A diferença entre estas duas MIB's reside nas hierarquias usadas para representar os objetos.
Na MIB da ISO são definidas três hierarquias: hierarquia de herança, hierarquia de nomeação e hierarquia de registro.
A hierarquia de herança ou de classes está relacionada às propriedades associadas a um determinado objeto. Dentro desta hierarquia diz-se que objetos da mesma classe possuem propriedades similares.
No caso da Internet não são usados os conceitos de classes de objetos e seus respectivos atributos. São definidos tipos de objetos. A definição de tipo de objetos contém cinco campos:
nome textual com o respectivo identificador de objeto (OBJECT IDENTIFIER), uma sintaxe ASN.1, uma descrição do objeto, o tipo de acesso e o status.

A hierarquia de nomeação ou de containment é usada para identificar instâncias de objetos.
Este tipo de hierarquia não é definido no caso da Internet. Finalmente tem-se a hierarquia de registro que é especificada em ambos padrões.

Tanto o SNMP como o CMIP suportam a mesma idéia de troca de mensagens entre gerente e agente e armazenamento das informações na MIB.
O SNMP devido a sua simplicidade e mais fácil de ser implementado. Em compensação, possui limitações de

desempenho que o CMIP não possui. Principalmente na área de segurança. Portanto o SNMP se adequa mais a sistemas de pequeno porte, onde se pode exigir menos de um sistema de gerenciamento.
O CMIP, devido a ser bem completo e bem projetado, e mais útil em sistemas de comunicação de grande porte, onde existem grandes quantidades de recursos a serem gerenciados. Em contraposição, em sistemas de pequeno porte, ele não se torna adequado devido a sua complexidade.

ESTUDO SOBRE RMON

Redes cliente/servidor estão, RMON – Remote Network Monitoring é um protocolo derivado do protocolo SNMP, foi criado pelos mesmos criadores do TCP/IP e do próprio SNMP.
Tecnologias como RMON pode dar ao administrador uma possibilidade maior de trabalhar proativamente quanto aos problemas da rede ao invés da reativa(atual) onde o problema ocorre para após isso corrigi-lo. Isto se torna possível devido ao suporte de estatísticas e dados em tempo-real. RMON2 (RMON versão2) permite um monitoramento até o nível de aplicação (RMON versão 1 permitia monitoramente somente até a camada MAC) possibilitando coletar informações como a banda usada por uma determinada aplicação.
Possui, além dessa, muitas outras vantagens.
O padrão RMON foi desenvolvido no intuito de resolver questões que outros protocolos de gerenciamento não eram capazes. Com base nestas questões, a RFC 1757 define objetivos gerenciais que o padrão RMON deve observar, abaixo listado.

Introdução
O RMON é um padrão IETF. Portanto, não é uma solução proprietária. Na realidade, um só fabricante dificilmente irá implementar a solução RMON completa. No cenário do gerenciamento RMON, os equipamentos de rede carregam MIBs RMON, a rede transporta os dados, um sistema de gerenciamento aceita alarmes e notifica usuários, e uma ferramenta de análise RMON interage com os grupos RMON e seus dados.

RMON
Os dispositivos de gerenciamento remoto de redes, normalmente chamados de monitores ou sondas (probes), são instrumentos cuja existência é dirigida exclusivamente ao gerenciamento de redes. Geralmente, são independentes (standalone) e direcionam boa parte de seus recursos internos ao gerenciamento da rede a qual estão conectados.
Uma organização pode empregar vários destes dispositivos para o gerenciamento de sua redeum por segmento. Adicionalmente, os monitores podem ser utilizados para que um provedor de serviços de gerenciamento de rede possa acessar uma rede cliente, normalmente separada geograficamente.
Os objetos definidos na RFC 1757 são objetos de interface entre agentes RMON e aplicações de gerenciamento RMON. Ainda que a maioria desses objetos sirva a qualquer tipo de gerenciamento de redes, alguns são específicos às redes Ethernet. A estrutura desta MIB permite que outros objetos sejam desenvolvidos para outros tipos de redes. Há uma expectativa de que futuras versões da RFC 1757 ou outros documentos definam extensões para outros tipos de redes, como FDDI ou Token Ring.

Operação Off-line
Existem situações em que uma estação de gerenciamento não estará em contato contínuo com seus dispositivos de gerenciamento remoto. Esta situação pode ocorrer como conseqüencia de projeto, a fim de que se reduzam os custos de comunicação, ou por falha da rede, quando a comunicação entre a estação de gerenciamento e o monitor fica comprometida em sua qualidade.
Por esta razão, a MIB RMON permite que um monitor seja configurado para realizar suas atividades de diagnóstico e coleta de dados estatísticos continuamente, mesmo quando a comunicação com a estação de gerenciamento seja impossível ou ineficiente. O monitor poderá então comunicar-se como a estação de gerenciamento quando uma condição excepcional ocorrer.
Assim, mesmo em circunstâncias em que a comunicação entre monitor e estação de gerenciamento não é contínua, as informações de falha, desempenho e configuração podem ser acumuladas de forma continua, e transmitidas à estação de gerenciamento conveniente e eficientemente quando necessário.

Monitoramento Proativo
Dados os recursos disponíveis no monitor, é normalmente desejável e potencialmente útil que ele execute rotinas de diagnóstico de forma contínua e que acumule os dados de desempenho da rede. O monitor estará sempre disponível no início de uma falha; assim, ele poderá notificar a estação de gerenciamento da falha, assim como armazenar informações estatísticas a seu respeito. Esta informação estatística poderá ser analizada pela estação de gerenciamento numa tentativa de diagnosticar as causas do problema.

Detecção e Notificação de Problemas
O monitor pode ser configurado para reconhecer condições, que, normalmente, são de erro e verificar pelas mesmas continuamente. No advento de uma destas condições, o evento pode ser registrado e as estações de gerenciamento notificadas de várias formas.
Valor Agregado aos Dados
Considerando o fato de que os dispositivos de gerenciamento remoto representam recursos dedicados exclusivamente a funções de gerenciamento, e considerando também que os mesmos localizam-se diretamente nas porções monitoradas da rede, pode-se dizer que estes dispositivos permitem a agregação de valor aos dados coletados. Por exemplo, indicando quais os hosts que geram a maior quantidade de tráfego ou erros, um dispositivo pode oferecer (à estação de gerenciamento) informações preciosas para a resolução de toda uma classe de problemas.

Gerenciamento Múltiplo
Uma organização pode ter mais de uma estação de gerenciamento para as várias unidades da empresa, para funções distintas, ou como tentativa de proporcionar

recuperação em caso de falha (crash recovery). Como tais ambientes são comuns na prática, um dispositivo de gerenciamento de rede remoto deverá ser capaz de lidar com múltiplas estações de gerenciamento concorrendo para a utilização de seus recursos.

O RMON (Remote Monitoring Network) é um protocolo que tem muito a prometer, ele é baseado na definição de limites de tolerância para a rede, é praticamente o snmp porém muito melhorado, com novas características e funções, o snmp só ia até o MAC Address da máquina, já o RMON continua e vai até a camada de aplicação do MIB, é muito importante pois possui mecanismos muito interessante para administrar a rede com uma melhor eficiência, possui atividades de diagnóstico e estatística quando uma estação estiver offline ou incomunicável enviando a informação a máquina gerenciadora que esta pode identificar as causas do problema ocorrido e proporcionar recuperação em casos de falha, chamados de crash recovery.